ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

ΣΤΡΑΤΗΓΙΚΗ ΕΡΓΑΣΙΑ

ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

ΜΕΣΟΛΟΓΓΙ

ΣΕΠΤΕΜΒΡΙΟΣ 2005

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

ΤΜΗΜΑ: *ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ*

Ε.Π.Δ.Ο

2005

ΟΙ ΣΠΟΥΔΑΣΤΕΣ

ΧΑΡΜΠΗΣ ΔΗΜΗΤΡΙΟΣ

ΗΛΙΟΠΟΥΛΟΣ ΣΠΗΛΙΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΓΡΗΓΟΡΙΟΣ ΜΠΕΛΗΓΙΑΝΝΗΣ

ΑΚΑΔΗΜΑΙΚΟ ΕΤΟΣ 2005-2006

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ 2ο
ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

ΠΙΝΑΚΕΣ ΚΑΙ ΣΧΗΜΑΤΑ

ΠΡΟΛΟΓΟΣ

Τα Δίκτυα Υπολογιστών και ειδικότερα το Διαδίκτυο (Internet) αποτελούν τη βάση ανάπτυξης της Κοινωνίας της Πληροφορίας. Βασικά χαρακτηριστικά των επικοινωνιακών υποδομών αποτελούν η ταχύτατη ανάπτυξη τους και η μεγάλη τους διεισδυτικότητα. Όλο και περισσότεροι οργανισμοί και πολίτες/χρήστες χρησιμοποιούν όλο και περισσότερες τηλεματικές εφαρμογές με «αιχμή του δόρατος» τον Παγκόσμιο Ιστό (WWW). Ως φυσικό επακόλουθο το πρόβλημα της ασφάλειας αναδεικνύεται ένας καθοριστικός παράγοντας επιτυχούς ανάπτυξης και λειτουργίας των σύγχρονων πληροφορικών περιβαλλόντων (υποδομές, επικοινωνιακές υπηρεσίες, υπηρεσίες προστιθέμενης αξίας).

Οι «απειλές» για την ασφάλεια ενός δικτύου μπορούν να προέλθουν από ένα μεγάλο αριθμό «πηγών», με πολλούς διαφορετικούς τρόπους, καλύπτοντας ένα ευρύτατο φάσμα περιπτώσεων. Η υπάρχουσα τάση για τη μεγαλύτερη δυνατή «αυτοματοποίηση» των επικοινωνιακών διαδικασιών αποτελεί ταυτόχρονα και την «αχίλλειο πτέρνα» πολλών διασυνδεδεμένων πληροφορικών συστημάτων.

Στη διόγκωση του προβλήματος της ασφάλειας «συμβάλλουν» επίσης οι σύγχρονες τεχνολογικές εξελίξεις. Ισχυρότεροι υπολογιστές και λογισμικό, πολλές εφαρμογές περιεχομένου και προστιθέμενης αξίας, ταχύτερα δίκτυα και συνοδευτικές υπηρεσίες καθώς και η ραγδαία αύξηση διασυνδεδεμένων υπολογιστών και έμπειρων χρηστών οδηγούν, μεταξύ των άλλων, και σε μια ραγδαία αύξηση των πιθανοτήτων για παραβιάσεις της ασφάλειας.

Πριν μια δεκαετία ένας κωδικός πρόσβασης (password) μπορούσε να εξασφαλίσει, σε μεγάλο βαθμό, την προστασία ενός συστήματος. Σήμερα η προσφερόμενη υπολογιστική ισχύς, η ταχύτητα επικοινωνίας και η ύπαρξη εξειδικευμένου λογισμικού για παραβιάσεις ασφάλειας (π.χ. λογισμικό ανίχνευσης κωδικών) δημιουργούν ένα τελείως διαφορετικό πεδίο και επιβάλλουν μια νέα συνολική και αυτοσυνεπή στρατηγική και αρχιτεκτονική ασφάλειας.

Δυστυχώς, στην πορεία ανάπτυξης των υποδομών πληροφορικής και των συνοδευτικών υπηρεσιών δε δόθηκε το ανάλογο βάρος στα θέματα της ασφάλειας. Ως ενδεικτικό παράδειγμα θα μπορούσε να αναφερθεί η αντιμετώπιση θεμάτων ασφάλειας από τις γλώσσες προγραμματισμού του WWW, όπως η ActiveX και η Java, όπου η πρώτη δεν παρέχει τις δυνατότητες χειρισμού παραμέτρων ασφάλειας που προσφέρει η δεύτερη.

Τέλος, πρέπει να τονισθεί ότι δυστυχώς η ανάγκη για ασφάλεια δε συμβαδίζει με την ίδια τη «φύση» του Διαδικτύου το οποίο γενικά χαρακτηρίζεται από χαλαρή διοίκηση/συντονισμό, τεχνολογική ετερογένεια, «πολιστική ποικιλία» και προσπάθεια για δημιουργία «ανοικτών» περιβαλλόντων με παροχή πρόσβασης στο μεγαλύτερο δυνατό αριθμό χρηστών.

Συμπερασματικά, θα μπορούσε να θεωρηθεί ότι η ανάγκη για συνεχή επαγρύπνηση σε θέματα ασφαλείας είναι το «τίμημα», μεταξύ των άλλων, που καλούμεθα να πληρώσουμε για τα πολλαπλά οφέλη που προσφέρει μια «δικτυωμένη κοινωνία»

ΜΕΡΟΣ 1ο

❖ ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΘΟΡΙΣΜΟΥ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

❖ ΑΠΕΙΛΕΣ & ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ 1ο

1.1 ΑΣΦΑΛΗ ΔΙΚΤΥΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ

1.2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

1.3 ΕΝΕΡΓΕΙΕΣ ΠΡΙΝ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

1.1 ΑΣΦΑΛΗ ΔΙΚΤΥΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ

Τι είναι ένα ασφαλές δίκτυο; Μπορεί ένα διαδίκτυο να γίνει ασφαλές; Αν και η έννοια του ασφαλούς δικτύου (secure network) γοητεύει τους περισσότερους χρήστες, τα δίκτυα δεν μπορούν απλώς να ταξινομηθούν σε ασφαλή και μη ασφαλή, επειδή ο όρος αυτός δεν είναι απόλυτος - κάθε οργανισμός ορίζει το επίπεδο πρόσβασης που επιτρέπει ή απαγορεύει. Για παράδειγμα, μερικοί οργανισμοί αποθηκεύουν δεδομένα τα οποία είναι πολύτιμα. Οι οργανισμοί αυτοί ορίζουν ως ασφαλές δίκτυο ένα σύστημα που εμποδίζει τους ξένους να αποκτούν πρόσβαση στους υπολογιστές του οργανισμού. Άλλοι οργανισμοί χρειάζεται να κάνουν τις πληροφορίες διαθέσιμες στους ξένους, αλλά να μην τους επιτρέπουν να κάνουν αλλαγές στα δεδομένα.

Οι οργανισμοί αυτοί μπορεί να ορίσουν ως ασφαλές ένα δίκτυο το οποίο επιτρέπει απεριόριστη πρόσβαση στα δεδομένα, αλλά περιλαμβάνει μηχανισμούς που εμποδίζουν τις αλλαγές από αναρμόδιους. Άλλες ομάδες πάλι, εστιάζουν την προσοχή τους στο να διατηρούν τις επικοινωνίες εμπιστευτικές. Αυτές ορίζουν ως ασφαλές ένα δίκτυο στο οποίο κανένας άλλος εκτός από τον τελικό αποδέκτη δεν μπορεί να υποκλέψει και να διαβάσει ένα μήνυμα. Τέλος, πολλοί μεγάλοι οργανισμοί χρειάζονται ένα σύνθετο ορισμό της ασφάλειας, που να επιτρέπει την πρόσβαση σε κάποια επιλεγμένα δεδομένα ή υπηρεσίες που έχει επιλέξει ο οργανισμός να κάνει δημόσια, ενώ εμποδίζει την πρόσβαση ή την τροποποίηση των ευαίσθητων δεδομένων και υπηρεσιών τα οποία διατηρούνται εμπιστευτικά.

Επειδή δεν υπάρχει απόλυτος ορισμός του ασφαλούς δικτύου, το πρώτο βήμα που πρέπει να κάνει ένας οργανισμός για να επιτύχει ένα ασφαλές σύστημα είναι να ορίσει την πολιτική ασφάλειάς (security policy) του. Η πολιτική αυτή δεν καθορίζει πώς θα επιτευχθεί η προστασία. Καθορίζει όμως ρητά και με σαφήνεια τα στοιχεία που πρέπει να προστατεύονται.

Ο ορισμός μιας πολιτικής ασφάλειας δικτύου είναι σύνθετη δουλειά. Η πολυπλοκότητα οφείλεται κυρίως στο ότι μια πολιτική ασφάλειας δικτύου δεν μπορεί να διαχωριστεί από την πολιτική ασφάλειας που ισχύει για τα υπολογιστικά συστήματα που είναι συνδεδεμένα στο δίκτυο. Ειδικότερα, ο ορισμός μιας πολιτικής για τα δεδομένα που περνούν από ένα δίκτυο δεν εγγυάται ότι τα δεδομένα θα είναι ασφαλή. Για παράδειγμα, ας υποθέσουμε ότι κάποια δεδομένα είναι αποθηκευμένα σε ένα αρχείο που επιτρέπεται η ανάγνωση του. Η ασφάλεια του δικτύου δεν μπορεί να εμποδίσει τους αναρμόδιους χρήστες που έχουν λογαριασμό στον υπολογιστή να πάρουν ένα αντίγραφο των δεδομένων. Επομένως, για να είναι αποτελεσματική μια πολιτική ασφάλειας, πρέπει να ισχύει πάντοτε. Η πολιτική πρέπει να ισχύει για τα δεδομένα που είναι αποθηκευμένα σε δίσκο, για τα δεδομένα που μεταφέρονται μέσω τηλεφωνικής γραμμής με ένα μόντεμ, για τις πληροφορίες που τυπώνονται σε χαρτί, για τα δεδομένα που μεταφέρονται σε φορητά μέσα, όπως μια δισκέτα, και για τα δεδομένα που μεταφέρονται μέσω ενός δικτύου υπολογιστών.

Η εκτίμηση του κόστους και της ωφέλειας των διαφόρων πολιτικών ασφάλειας κάνει επίσης το ζήτημα πιο σύνθετο. Συγκεκριμένα, μια πολιτική ασφάλειας δεν μπορεί να οριστεί παρά μόνο αν ο οργανισμός αντιλαμβάνεται την αξία των πληροφοριών του. Σε πολλές περιπτώσεις, η αξία των πληροφοριών είναι δύσκολο να εκτιμηθεί. Φανταστείτε, για παράδειγμα, μια απλή βάση δεδομένων μισθοδοσίας, η οποία περιέχει μια εγγραφή για κάθε υπάλληλο, τις ώρες που εργάστηκε ο υπάλληλος, και την αμοιβή του.

Η ευκολότερη άποψη της αξιολόγησης είναι να εκτιμηθεί το κόστος αντικατάστασης. Δηλαδή, μπορεί να υπολογιστούν οι ώρες εργασίας που χρειάζονται για να ξαναδημιουργηθεί ή να επαληθευτεί το περιεχόμενο της βάσης δεδομένων (π.χ. με την αποκατάσταση των

δεδομένων από ένα εφεδρικό αντίγραφο ή με την πραγματοποίηση της εργασίας που χρειάζεται για να συλλεχθούν οι πληροφορίες). Μια δεύτερη άποψη της αξιολόγησης είναι να εκτιμηθεί το παθητικό που μπορεί να προκληθεί στον οργανισμό αν οι πληροφορίες είναι λανθασμένες. Για παράδειγμα, αν ένα αναρμόδιο άτομο αυξήσει τις αμοιβές σε μια βάση δεδομένων μισθοδοσίας, η εταιρία θα μπορούσε να επιβαρυνθεί με οποιοδήποτε κόστος αν οι υπάλληλοι θα πληρώνονταν περισσότερο.

Μια τρίτη άποψη της αξιολόγησης είναι το έμμεσο κόστος που θα μπορούσε να προκληθεί από παραβιάσεις της ασφάλειας. Για παράδειγμα, αν οι πληροφορίες μισθοδοσίας κοινοποιηθούν, μπορεί οι ανταγωνιστές να επιλέξουν να προσλάβουν κάποιους εργαζόμενους, με αποτέλεσμα ένα κόστος πρόσληψης και εκπαίδευσης αντικαταστατών, καθώς και αυξήσεις αμοιβών για να κρατήσει η εταιρία κάποιους άλλους υπαλλήλους.

1.2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

1.2.1 ΤΙ ΕΙΝΑΙ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Μια πολιτική ασφάλειας είναι ένα έγγραφο υψηλού επιπέδου που επιτρέπει σε μια οργάνωση και τη διοικητική της ομάδα να χαρακτηρίσει τους πολύ σαφείς και κατανοητούς στόχους, τους σκοπούς, τους κανόνες και τις επίσημες διαδικασίες που βοηθούν να καθορίσουν τη γενική στάση και την αρχιτεκτονική ασφάλειας για την εν λόγω οργάνωση.

Χωρίς την ύπαρξη πολιτικής ασφάλειας, δεν υπάρχει ένα γενικό πλαίσιο για την ασφάλεια. Με την πολιτική ασφάλειας ορίζεται ποια συμπεριφορά είναι επιτρεπόμενη μέσα στον οργανισμό ως προς την χρήση των προσφερόμενων υπηρεσιών, μέσα από διαδικασίες που πρέπει να ακολουθηθούν από όλους.

Η πολιτική ασφάλειας είναι μια καλή μέθοδος για την δημιουργία συναντίληψης ανάμεσα στα στελέχη του οργανισμού.

Μια πολιτική ασφάλειας πρέπει επίσης να δημιουργηθεί με πολλή σκέψη και ειδική επεξεργασία. Θα μπορούσε να καταστηθεί μια πολιτική ασφάλειας που να είναι πάρα πολύ περιοριστική. Εάν ναι, μπορεί να προκληθεί πολύ πίεση στους υπαλλήλους της εταιρίας, οι οποίοι μπορούν να είναι εξοικειωμένοι με έναν άλλο τρόπο εργασίας, και μπορεί να τους πάρει πολύ χρόνο σε μια πιο περιοριστική στάση βασισμένη στην πολιτική αυτή.

Κάθε επιχείρηση έχει διαφορετικούς υπολογιστικούς πόρους, διαφορετική κουλτούρα και διαφορετική υποδομή. Οι υπεύθυνοι ανάπτυξης της πολιτικής ασφάλειας θα πρέπει:

- ✓ Να λάβουν υπόψη τους στόχους και την κατεύθυνση της επιχείρησης. Ενδέχεται διαφορετικά τμήματα της επιχείρησης να έχουν διαφορετικές απαιτήσεις στα θέματα ασφάλειας και επομένως όλες οι επιμέρους ιδιαιτερότητες πρέπει να ληφθούν υπόψη.
- ✓ Να αναπτύξουν την πολιτική ασφάλειας έτσι ώστε να ανταποκρίνεται στους κανονισμούς, στους νόμους και στην γενικότερη πολιτική που ακολουθεί η επιχείρηση.
- ✓ Να αναπτύξουν την πολιτική ασφάλειας λαμβάνοντας υπόψη τις γενικότερες επιπτώσεις που δημιουργεί ένα ανοικτό δίκτυο. Συγκεκριμένα, θα πρέπει να αντιμετωπιστούν ενδεχόμενα προβλήματα ασφάλειας που θα δημιουργήσει μία

εξωτερική εισβολή στην επιχείρηση καθώς και προβλήματα ασφαλείας που θα δημιουργήσει κάποιος χρήστη του δικτύου της επιχείρησης σε ένα εξωτερικό site.

Η πολιτική ασφάλειας δικτύου αποτελεί ένα ιδιαίτερα χρήσιμο έγγραφο διότι σε συνδυασμό με άλλες πολιτικές της επιχείρησης αποτελεί οδηγό για την αντιμετώπιση των προβλημάτων ασφαλείας και αναμφίβολα βοηθά στη λήψη αποφάσεων. Σε περίπτωση που παρατηρηθεί κάποια εισβολή, η πολιτική ασφαλείας δικτύου εμποδίζει την πρόχειρη αντιμετώπιση του θέματος.

1.2.2 ΠΟΙΟΙ ΕΜΠΛΕΚΟΝΤΑΙ ΣΤΟΝ ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Μια πολιτική ασφαλείας για να είναι κατάλληλη για τον οργανισμό θα πρέπει να είναι αποδεκτή από όλους τους εργαζόμενους. Επίσης θα πρέπει να υπάρχει υποστήριξη της πολιτικής και από τη διεύθυνση του οργανισμού ώστε να επιτύχει τους στόχους της. Οι ομάδες εργαζομένων που εμπλέκονται σε μια πολιτική ασφάλειας είναι:

- ***Οι απλοί χρήστες*** - η πολιτική ασφαλείας αφορά αυτούς επί το πλείστον.
- ***Προσωπικό υποστήριξης*** - είναι αυτοί που θα υλοποιήσουν και θα υποστηρίξουν την πολιτική ασφάλειας.
- ***Διοικητικό προσωπικό*** - καθορίζουν το βαθμό προστασίας των περισσότερων δεδομένων και αναλαμβάνουν το οικονομικό κόστος της πολιτικής που θα υλοποιηθεί.
- ***Νομικοί σύμβουλοι*** - αυτοί που ενδιαφέρονται για τη φήμη και τη νομική κάλυψη του οργανισμού.

1.2.3 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Οι αποφάσεις που λαμβάνονται για την ασφάλεια ενός δικτύου από τον διαχειριστή του, καθορίζουν το πόσο ασφαλές είναι ένα δίκτυο καθώς και την ευκολία στη χρήση του.

Καταρχήν θα πρέπει να αποφασιστεί τι είναι σκόπιμο να διαφυλαχτεί. Όταν γίνει αυτό θα πρέπει να οριστούν οι περιορισμοί που θα πρέπει να τεθούν ώστε να έχουμε το επιθυμητό αποτέλεσμα.

Οι στόχοι καθορίζονται από τους ακόλουθους παράγοντες:

1) Προσφερόμενες υπηρεσίες σε σχέση με την ασφάλεια του δικτύου. Υπάρχουν περιπτώσεις που η χρήση κάποιων υπηρεσιών αυξάνει τον κίνδυνο για την άρση της ασφάλειας ενός δικτύου, με αποτέλεσμα το κόστος των υπηρεσιών αυτών να είναι μεγαλύτερο από τα οφέλη τους. Σε τέτοιες περιπτώσεις είναι προτιμότερη η κατάργηση της υπηρεσίας.
2) Ευκολία χρήσης σε σχέση με τη προσφερόμενη ασφάλεια. Το ευκολότερο σύστημα στη χρήση είναι αυτό που προσφέρει άμεση πρόσβαση χωρίς την ύπαρξη συνθηματικών. Παρόλα αυτά ένα τέτοιο σύστημα δεν προσφέ-

ρει καμία απολύτως ασφάλεια. Με την χρήση συνθηματικών (password) το σύστημα γίνεται λίγο πιο δύσκολο αφού κάθε χρήστης θα πρέπει να θυμάται τον κωδικό του, αλλά ταυτόχρονα γίνεται και πιο ασφαλές.

3) Κόστος ασφάλειας ενάντια στον κίνδυνο απώλειας. Υπάρχουν διάφορα είδη που προσδιορίζουν το κόστος της ασφάλειας όπως:

- Κόστος αγοράς υλικού ή λογισμικού, όπως firewalls και on-time password generators
- Απόδοση (η κωδικοποίηση και η αποκωδικοποίηση χρειάζονται κάποιο χρόνο) καθώς και ευκολία στη χρήση.

Υπάρχουν επίσης διάφορα επίπεδα κινδύνου όπως:

- Άρση του απορρήτου (π.χ. ανάγνωση πληροφορίας από τρίτους),
- Απώλεια δεδομένων (διαγραφή δεδομένων) ή
- Απώλεια υπηρεσιών (χρήση των πηγών του δικτύου, άρνηση πρόσβασης στο δίκτυο κ.α.).

Για την υλοποίηση της ασφάλειας του δικτύου θα πρέπει να ληφθούν υπόψη όλα τα παραπάνω.

1.2.4 ΤΑ ΣΥΣΤΑΤΙΚΑ ΤΗΣ ΚΑΛΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Μια πολιτική ασφάλειας θα πρέπει να είναι:

Υλοποιήσιμη: Να υπάρχουν ρεαλιστικοί κανόνες διαχείρισης των συστημάτων για κάθε τμήμα του οργανισμού, οδηγίες χρήσης των διάφορων πόρων, εγκατεστημένα συστήματα ασφάλειας.

Θα πρέπει να ακολουθείται απ' όλους: Οι χρήστες θα πρέπει να κατανοήσουν πως δε γίνονται παρακάμψεις για τη διευκόλυνση τους. Θα πρέπει οι ίδιοι να προσαρμόσουν τις καθημερινές δραστηριότητες τους στους κανόνες ασφάλειας. Δεν θα πρέπει όμως να είναι και υπερβολικά αυστηροί γιατί τότε οι χρήστες θα προσπαθούν να βρουν τρόπους για να ξεπεράσουν τους κανόνες.

Ευέλικτη: Για να είναι βιώσιμη μια πολιτική ασφάλειας θα πρέπει να εξαρτάται από το υλικό και το λογισμικό που υπάρχει, ώστε να μπορεί να αναπροσαρμόζει τους κανόνες της σύμφωνα με τις προδιαγραφές τους. Επίσης θα πρέπει να αναγνωρίζει τις εξαιρέσεις που είναι δυνατό να γίνουν στους κανόνες ασφάλειας ανάλογα με τις ανάγκες που θα παρουσιαστούν. Για παράδειγμα ο διαχειριστής ενός συστήματος μπορεί να χρειαστεί τον κωδικό πρόσβασης κάποιου χρήστη για ένα σύστημα. Θα πρέπει να ισοσταθμίζει την προστασία του οργανισμού με την παραγωγικότητα. Αν οι κανόνες είναι πολύ αυστηροί οι χρήστες θα βρουν τρόπους να μην τους εφαρμόζουν. Οι τεχνικοί έλεγχοι δεν είναι πάντα εφικτοί.

Αναβαθμίσιμη: Οι κανόνες που τίθενται θα πρέπει να αναπροσαρμόζονται και να ακολουθούν την εξέλιξη του οργανισμού.

Κατανοητή: Οι άνθρωποι που την διαβάζουν πρέπει να είναι σε θέση να συμμορφωθούν εύκολα. Πρέπει να εξασφαλίζεται ότι δεν περιέχει πολύ τεχνολογική φλυαρία έτσι ώστε να μπορεί να υποστηριχτεί από έναν τελικό χρήστη.

Την πολιτική ασφάλειας που θα εφαρμόσουμε πρέπει να έχουν την ευκαιρία να την σχολιάσουν και όσοι θα δεχτούν τις επιπτώσεις της.

1.3 ΕΝΕΡΓΕΙΕΣ ΠΡΙΝ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

1.3.1 ΑΞΙΟΛΟΓΗΣΗ ΤΟΥ ΚΙΝΔΥΝΟΥ

Ένας από τους σημαντικότερους λόγους για τον οποίο δημιουργείται μια πολιτική ασφάλεια δικτύων ή υπολογιστών, είναι να εξασφαλίσει ότι οι προσπάθειες που ξοδεύονται στην ασφάλεια παράγουν αποτελεσματικά οφέλη. Αν και αυτό μπορεί να φανεί προφανές, είναι πιθανόν να υπάρχει παραπλάνηση για το που απαιτείται η προσπάθεια. Σαν παράδειγμα, υπάρχει πολλή δημοσιότητα για τους εισβολείς επάνω σε συγκροτήματα ηλεκτρονικών υπολογιστών, ωστόσο οι περισσότερες έρευνες για την ασφάλεια υπολογιστών δείχνουν ότι για τις περισσότερες οργανώσεις, η απώλεια από "εσωτερικά μέλη" είναι πραγματικά πολύ μεγαλύτερη.

Η ανάλυση κινδύνου περιλαμβάνει τον καθορισμό του τι πρέπει να προστατευτεί, από τι πρέπει να προστατευτεί, και πώς να προστατευτεί. Η διαδικασία εξετάζει όλους τους κινδύνους και τους ταξινομεί ανάλογα με το επίπεδο σοβαρότητας του κάθε κινδύνου. Αυτή η διαδικασία περιλαμβάνει την παραγωγή αποδοτικών οικονομικών αποφάσεων σχετικά με αυτό που πρέπει να προστατευτεί. Η παλαιά παροιμία ασφάλειας λέει ότι δεν πρέπει να ξοδευτούν περισσότερα, για να προστατευτεί κάτι, από ότι είναι η πραγματική του αξία.

Μια πλήρης επεξεργασία της ανάλυσης κινδύνου είναι έξω από το πεδίο αυτού του εγγράφου. Εντούτοις, υπάρχουν δύο στοιχεία μιας ανάλυσης κινδύνου που θα πρέπει να καλυφθούν εν συντομία στα επόμενα δύο τμήματα:

1. Προσδιορισμός των πόρων

2. Προσδιορισμός των απειλών

Για κάθε προτέρημα, οι βασικοί στόχοι της ασφάλειας είναι η διαθεσιμότητα, η εμπιστευτικότητα, και η ακεραιότητα. Κάθε απειλή πρέπει να εξεταστεί στοχεύοντας στο πώς η απειλή θα μπορούσε να έχει επιπτώσεις σε αυτές τις περιοχές.

1.3.1.1 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΠΟΡΩΝ

Ένα βήμα σε μια ανάλυση κινδύνου είναι να προσδιοριστούν όλα τα πράγματα που έχουν ανάγκη να προστατευθούν. Μερικά πράγματα είναι προφανή, όπως όλα τα διάφορα κομμάτια του υλικού, αλλά μερικά αγνοούνται, όπως οι άνθρωποι που χρησιμοποιούν

πραγματικά τα συστήματα. Το ουσιαστικό σημείο είναι να απαριθμηθούν όλα τα πράγματα που θα μπορούσαν να επηρεαστούν από ένα πρόβλημα ασφάλειας.

Η κατηγοριοποίηση των πόρων που θα προστατευθούν έχει ως εξής:

1) ***Υλικό:*** CPU's, πίνακες, πληκτρολόγια, τερματικά, τερματικοί σταθμοί, προσωπικοί υπολογιστές, εκτυπωτές, μονάδες δίσκων, γραμμές επικοινωνίας, κεντρικοί υπολογιστές, δρομολογητές.

2) ***Λογισμικό:*** προγράμματα πηγής, προγράμματα αντικειμένου, utilities, διαγνωστικά προγράμματα, λειτουργικά συστήματα, προγράμματα επικοινωνίας.

3) ***Στοιχεία:*** που επιδέχονται επεξεργασία κατά τη διάρκεια της εκτέλεσης, που αποθηκεύονται on-line, που αρχειοθετούνται off-line, backups, λογιστικού ελέγχου, βάσεις δεδομένων, μέσα επικοινωνίας κατά τη μεταφορά.

4) ***Άνθρωποι:*** οι χρήστες, άνθρωποι που πρέπει να λειτουργούν τα συστήματα.

5) ***Τεκμηρίωση:*** στα προγράμματα, υλικό, συστήματα, τοπικές διοικητικές διαδικασίες.

6) ***Προμήθειες:*** έγγραφο, μορφές, ταινίες, μαγνητικά μέσα.

1.3.1.2 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΑΠΕΙΛΩΝ

Μόλις προσδιοριστούν οι πόροι που απαιτούν προστασία, είναι απαραίτητο να προσδιοριστούν οι πιθανές απειλές τους. Οι απειλές μπορούν κατόπιν να εξεταστούν για να καθορίσουν ποια πιθανότητα απώλειας υπάρχει. Αυτό βοηθάει κάποιον στο να εξετάσει από ποιες απειλές προσπαθεί να προστατεύσει τους πόρους του.

1.3.2 ΑΝΑΘΕΩΡΗΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Η αξιολόγηση του κινδύνου δεν πρέπει να γίνει μόνο μία φορά και να ξεχαστεί έπειτα. Αντιθέτως, πρέπει να ενημερώνεται η αξιολόγησή περιοδικά. Επιπλέον, η αξιολόγηση του κινδύνου πρέπει να ξαναγίνετε όποτε υπάρχει μια σημαντική αλλαγή στη λειτουργία ή τη δομή του οργανισμού. Κατά συνέπεια, εάν αναδιοργανώνετε, μεταφέρεστε προς ένα νέο κτίριο, αλλάζετε τους προμηθευτές, ή άλλες σημαντικές αλλαγές, πρέπει να επαναξιολογήσετε τις απειλές και τις πιθανές απώλειες.

1.3.3 ΑΝΑΛΥΣΗ ΚΟΣΤΟΥΣ – ΟΦΕΛΟΥΣ (COST BENEFIT ANALYSIS)

Ο βασικός κανόνας σε θέματα ασφαλείας είναι: ***η οικονομική αξία των μέτρων ασφάλειας για την προστασία ενός περιουσιακού στοιχείου δεν θα πρέπει να υπερβαίνει την αξία του.*** Εάν η προστασία ενός περιουσιακού στοιχείου κοστίζει περισσότερο από ότι η αντικατάστασή του σε περίπτωση παραβίασης, τότε δεν πρέπει να ληφθούν μέτρα ασφαλείας. Ενδέχεται κάποια περιουσιακά στοιχεία της επιχείρησης να έχουν σχετικά μικρή αξία αλλά να κριθεί σκόπιμη η επιβολή μέτρων ασφάλειας, ενώ λόγω πολύ υψηλού κόστους να μην πρέπει να χρησιμοποιηθούν μέτρα ασφάλειας για τα πιο σημαντικά περιουσιακά στοιχεία της επιχείρησης.

1.3.4 ΕΠΙΛΟΓΗ ΜΟΝΤΕΛΟΥ DENY ALL/ALLOW ALL

Υπάρχουν δυο διαμετρικά αντίθετες φιλοσοφίες που μπορούν να υιοθετηθούν κατά το σχεδιασμό της ασφάλειας ενός δικτυακού τόπου (site). Η φιλοσοφία που θα ακολουθηθεί εξαρτάται από το δικτυακό τόπο και τις ανάγκες του [RFC 2196].

Στο πρώτο μοντέλο προτείνεται η κατάργηση όλων των υπηρεσιών και η επιλεκτική ενεργοποίηση τους ανάλογα με τις εκάστοτε ανάγκες. Το μοντέλο αυτό γνωστό σαν «deny all» είναι πιο ασφαλές αλλά και πιο δύσκολο στην εφαρμογή του. Για να εφαρμοστεί το μοντέλο αυτό απαιτείται καλή γνώση των υπηρεσιών και των αντίστοιχων πρωτοκόλλων.

Το δεύτερο μοντέλο γνωστό σαν «allow all», είναι πολύ πιο εύκολο στην εφαρμογή του αλλά και λιγότερο ασφαλές από τον τύπο «deny all». Στο μοντέλο αυτό ενεργοποιούνται από την αρχή όλες οι υπηρεσίες και επιτρέπονται όλα τα πρωτόκολλα σε επίπεδο δικτύου. Ανάλογα με τα προβλήματα που παρουσιάζονται κατά την εφαρμογή αυτού του μοντέλου γίνονται περιορισμοί τόσο σε επίπεδο host όσο και σε επίπεδο δικτύου.

Σε ένα δικτυακό τόπο είναι δυνατό να ακολουθηθούν και τα δυο μοντέλα. Για παράδειγμα το μοντέλο «allow all» μπορεί να υιοθετηθεί για την επικοινωνία δύο τοπικών δικτύων ενώ το δεύτερο μοντέλο «deny all» για τη σύνδεση ενός δικτυακού τόπου με το Διαδίκτυο.

1.3.5 ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η επιτροπή ασφαλείας αρχικά θα πρέπει να επιλέξει τη βάση πάνω στην οποία θα δομηθεί η πολιτική ασφάλειας [Site1]. Πρέπει να επιλέξει στρατηγική ασφάλειας άμεσα συνδεδεμένη με το επίπεδο επικινδυνότητας που χαρακτηρίζει την επιχείρηση. Με τον όρο στρατηγική ασφάλειας ορίζεται η γενικότερη αντίληψη που έχει η επιχείρηση για το θέμα της ασφάλειας.

Ακολούθως παρουσιάζονται οι διάφορες στρατηγικές ασφάλειας [Chap95]:

LEAST PRIVILEGE

Η στρατηγική αυτή βασίζεται στην αρχή ότι η εξουσιοδότηση δικαιωμάτων πρόσβασης θα πρέπει να γίνεται μόνο όταν είναι απαραίτητη. Επομένως, όσοι απαιτείται να έχουν

πρόσβαση στα συστήματα της επιχείρησης θα πρέπει να έχουν μόνο τα δικαιώματα πρόσβασης που είναι απαραίτητα για την διεκπεραίωση της εργασίας τους.

Η υιοθέτηση της στρατηγικής αυτής περιορίζει τις επιθέσεις στα υπολογιστικά συστήματα της επιχείρησης. Επίσης, μειώνονται οι τυχόν απώλειες σε περίπτωση που επιτύχει μη εξουσιοδοτημένη πρόσβαση.

CHOKE POINT

Choke Point είναι ένα συγκεκριμένο σημείο από όπου ελέγχεται η εισερχόμενη και εξερχόμενη κίνηση του δικτύου της επιχείρησης.

Πολλές επιχειρήσεις υιοθετούν την στρατηγική αυτή χρησιμοποιώντας πυρότοιχους (firewalls) στους οποίους συγκεντρώνεται και ελέγχεται η κίνηση του δικτύου. Βασική αδυναμία της στρατηγικής αυτής είναι ότι στην περίπτωση που παραβιαστεί το choke point, το οποίο αποτελεί ασπίδα προστασίας, τότε τα συστήματα της επιχείρησης είναι πλέον εκτεθειμένα σε σοβαρό κίνδυνο. Επίσης, τα choke point αποτελούν σημείο συνωστισμού και επομένως η επιχείρηση θα πρέπει να πιστοποιήσει ότι υπάρχει αρκετό εύρος ζώνης (bandwidth) για την υιοθέτηση της στρατηγικής αυτής, αποφεύγοντας συμφόρηση της κίνησης.

DEFENCE IN DEPTH

Η στρατηγική αυτή υποστηρίζει το συνδυασμό πολλών μηχανισμών ασφάλειας. Στόχος είναι να αντιμετωπιστούν οι αδυναμίες που παρουσιάζουν τα συστήματα ασφάλειας χρησιμοποιώντας ποικιλία τέτοιων συστημάτων.

Για παράδειγμα σε περίπτωση που κάποιος επιτιθέμενος ανιχνεύσει μία ευπάθεια σε κάποιο πυρότοιχο τύπου Α, εάν η επιχείρηση χρησιμοποιεί πυρότοιχους διαφορετικού τύπου σε σειριακή τοποθέτηση τότε μπορεί να αντιμετωπίσει αυτή την ευπάθεια.

FAIL SAFE STANCE

Στόχος της στρατηγικής αυτής είναι το σύστημα να μεταβαίνει σε ασφαλή κατάσταση σε περίπτωση αποτυχίας. Για παράδειγμα, σε περίπτωση που παρατηρηθεί μη ομαλή λειτουργία του πυρότοιχου που χρησιμοποιείται, τότε θα πρέπει αυτόματα να διακόπτεται η ροή της κίνησης από και προς το δίκτυο της επιχείρησης.

LOW PROFILE

Η επιχείρηση θα πρέπει να επιδιώκει να είναι στην «αφάνεια» εννοώντας ότι όσο περισσότερο ορατή είναι η επιχείρηση μέσω ενός ανοικτού δικτύου τόσο περισσότερο εκτίθεται σε κίνδυνο.

Για παράδειγμα πολλές επιχειρήσεις διατηρούν μυστικό τον αριθμό του dial-in modem που χρησιμοποιούν και επιβάλλουν αλλαγή του αριθμού αυτού περιοδικά. Προφανώς η υιοθέτηση της στρατηγικής αυτής δεν αποτελεί βάση για μακροπρόθεσμο σχεδιασμό ασφάλειας, αλλά μπορεί να χρησιμοποιηθεί σε συνδυασμό με κάποια άλλη στρατηγική.

1.3.6 ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΙΣΒΟΛΩΝ

Η επιτροπή ασφάλειας θα πρέπει να επιλέξει την στρατηγική που θα ακολουθήσει η επιχείρηση σε περίπτωση εισβολής. Η επιτροπή ασφαλείας μπορεί να επιλέξει μία πολιτική

αντιμετώπισης που θα ισχύει για όλους τους τύπους των εισβολών ή ενδέχεται να επιλέξει διαφορετική στρατηγική αντιμετώπιση ανάλογα με τον τύπο κάθε εισβολής. Η δεύτερη επιλογή θεωρείται πιο ασφαλής ιδιαίτερα για περιβάλλοντα υψηλού κινδύνου.

Οι στρατηγικές αντιμετώπισης εισβολών είναι [RFC 1244]:

◈ Protect and Proceed

Στόχος είναι να διακοπεί άμεσα η εισβολή, να εκτιμηθεί το κόστος και να γίνει επαναφορά του συστήματος. Προκειμένου να κατασταλεί άμεσα η εισβολή διακόπτεται προσωρινά η πρόσβαση στο δίκτυο ή λαμβάνονται άλλα δραστικά μέτρα. Το μειονέκτημα της πολιτικής αυτής είναι ότι η επιχείρηση αδυνατεί να εντοπίσει την ευπάθεια του συστήματος και επομένως ο επιτήδειος εισβολέας μπορεί να την εκμεταλλευθεί μεταγενέστερα.

Τα κριτήρια βάσει των οποίων θα πρέπει να επιλεγεί η συγκεκριμένη πολιτική αντιμετώπισης εισβολών είναι τα εξής:

- *Εάν τα περιουσιακά στοιχεία της επιχείρησης δεν είναι καλά προστατευμένα*
- *Εάν η περαιτέρω πρόσβαση του εισβολέα δημιουργεί μεγάλο οικονομικό ρίσκο για την επιχείρηση*
- *Εάν η επιχείρηση δεν είναι διατεθειμένη να επιβάλει κυρώσεις ή να προχωρήσει σε ποινική δίωξη του εισβολέα*
- *Εάν οι γνώσεις των χρηστών σε θέματα ασφαλείας δεν είναι ικανοποιητικές και επομένως η εργασία τους δημιουργεί ευπάθειες στο υπολογιστικό σύστημα της επιχείρησης.*

◈ Pursue and Prosecute

Κύριος στόχος είναι να επιτρέψουν στον εισβολέα να συνεχίσει τις κακόβουλες δραστηριότητές του προκειμένου να προσδιορίσουν την ταυτότητα του. Προφανώς, μετά τον εντοπισμό του εισβολέα η επιχείρηση μπορεί να προχωρήσει στη επιβολή κυρώσεων. Βασικό μειονέκτημα της στρατηγικής αυτής είναι ότι ενδέχεται να γίνει εκτεταμένη ζημία και η ταυτότητα του εισβολέα να παραμείνει άγνωστη.

Τα κριτήρια βάσει των οποίων θα πρέπει να επιλεγεί η συγκεκριμένη πολιτική αντιμετώπισης εισβολών είναι τα εξής:

- *Εάν τα περιουσιακά στοιχεία και τα υπολογιστικά συστήματα της επιχείρησης είναι καλά προστατευμένα.*
- *Εάν υπάρχουν διαθέσιμα καλά αντίγραφα ασφαλείας (back-ups).*
- *Εάν πρόκειται για εισβολές που εμφανίζονται με μεγάλη συχνότητα και ένταση.*
- *Εάν η επιχείρηση αποτελεί πόλο έλξης για τους εισβολείς.*
- *Εάν η επιχείρηση είναι διατεθειμένη να αναλάβει το οικονομικό κόστος της περαιτέρω εισβολής.*
- *Εάν η πρόσβαση του εισβολέα μπορεί να ελεγχθεί.*
- *Εάν τα εργαλεία παρακολούθησης είναι ικανοποιητικά και επομένως επιτρέπουν την συλλογή αποδεικτικών στοιχείων για την ποινική δίωξη του εισβολέα.*
- *Εάν οι γνώσεις του προσωπικού ασφάλειας αναφορικά με το λειτουργικό σύστημα και τα δίκτυα υπολογιστών είναι επαρκείς.*
- *Εάν η διοίκηση της επιχείρησης είναι διατεθειμένη να επιβάλει κυρώσεις και να διώξει ποινικά τον εισβολέα.*

- *Εάν οι διαχειριστές του συστήματος γνωρίζουν ποια στοιχεία μπορούν να στοιχειοθετήσουν κατηγορητήριο για τον εισβολέα.*

ΚΕΦΑΛΑΙΟ 2ο

2.1 ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

2.2 ΑΠΕΙΛΕΣ

2.3 ΤΑ ΒΑΣΙΚΟΤΕΡΑ ΕΙΔΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΔΙΚΤΥΩΝ

2.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΠΙΘΕΣΕΩΝ ΠΟΥ ΕΧΟΥΝ ΣΥΜΒΕΙ ΔΙΕΘΝΩΣ

2.1 ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Μια απλή κατηγοριοποίηση των υπηρεσιών ασφαλείας είναι η εξής [Stall99]:

Εμπιστευτικότητα

Η εμπιστευτικότητα είναι η προστασία των στοιχείων που μεταδίδονται από τις παθητικές επιθέσεις. Όσον αφορά την αποκάλυψη του περιεχομένου των μηνυμάτων, διάφορα επίπεδα προστασίας μπορούν να προσδιοριστούν. Η ευρύτερη υπηρεσία προστατεύει όλα τα στοιχεία των χρηστών που μεταδίδονται μεταξύ δύο χρηστών για μια χρονική περίοδο. Παραδείγματος χάριν, εάν ένα εικονικό κύκλωμα έχει δημιουργηθεί μεταξύ δύο συστημάτων, αυτή η ευρεία προστασία θα απέτρεπε την απελευθέρωση οποιωνδήποτε στοιχείων των χρηστών που μεταδίδονται πέρα από το εικονικό κύκλωμα. Πιο συγκεκριμένες μορφές αυτής της υπηρεσίας μπορούν επίσης να καθοριστούν, συμπεριλαμβανομένης της προστασίας ενός απλού μηνύματος ή ακόμα και ειδικών τομέων μέσα σε ένα μήνυμα. Αυτές οι μορφές είναι λιγότερο χρήσιμες από την ευρεία προσέγγιση και μπορεί ακόμη να είναι πιο σύνθετες και πιο ακριβές για να εφαρμοστούν.

Η άλλη πτυχή της εμπιστευτικότητας είναι η προστασία της κυκλοφοριακής ροής από την ανάλυση. Αυτό απαιτεί ότι ένας επιτιθέμενος δεν είναι σε θέση να παρατηρήσει την πηγή και τον προορισμό, τη συχνότητα, το μήκος ή και άλλα χαρακτηριστικά της κυκλοφορίας σε μια επικοινωνία.

Πιστοποίηση

Η υπηρεσία πιστοποίησης ενδιαφέρεται για τη βεβαίωση ότι μια επικοινωνία είναι αυθεντική. Στην περίπτωση ενός απλού μηνύματος, όπως ένα σήμα προειδοποίησης ή συναγερμού, η λειτουργία της υπηρεσίας πιστοποίησης είναι να βεβαιώσει τον παραλήπτη ότι το μήνυμα είναι από την πηγή από την οποία υποστηρίζει ότι είναι. Στην περίπτωση μιας τρέχουσας αλληλεπίδρασης, όπως η σύνδεση ενός τερματικού με έναν κεντρικό υπολογιστή δικτύου, δύο πτυχές περιλαμβάνονται. Κατ' αρχάς, κατά την διάρκεια της έναρξης σύνδεσης, η υπηρεσία βεβαιώνει ότι οι δύο οντότητες είναι αυθεντικές (δηλαδή ότι κάθε μια είναι η οντότητα που υποστηρίζει ότι είναι). Δεύτερον, η υπηρεσία πρέπει να βεβαιώσει ότι η σύνδεση δεν παρεμποδίζεται κατά τέτοιο τρόπο ώστε μια τρίτη οντότητα να μπορεί να εισχωρήσει κρυφά, υποδυόμενη μια από τις δύο νόμιμες συμβαλλόμενες ομάδες, για τους σκοπούς της αναρμόδιας μετάδοσης ή λήψης.

Ακεραιότητα

Όπως με την εμπιστευτικότητα, η ακεραιότητα μπορεί να ισχύσει για μια ροή μηνυμάτων, για ένα απλό μήνυμα ή για επιλεγμένους τομείς μέσα σε ένα μήνυμα. Και πάλι, η πιο χρήσιμη και απλή προσέγγιση είναι η συνολική προστασία της ροής.

Μια υπηρεσία ακεραιότητας επικεντρωμένη προς τη σύνδεση, που εξετάζει μια ροή μηνυμάτων, βεβαιώνει ότι τα μηνύματα παραλαμβάνονται όπως στέλνονται, χωρίς το διπλασιασμό, εισαγωγή, τροποποίηση, επαναποστολή ή επανάληψη. Η καταστροφή των δεδομένων καλύπτεται επίσης από αυτή την υπηρεσία. Κατά συνέπεια, η προσανατολισμένη προς τη σύνδεση υπηρεσία ακεραιότητας εξετάζει και την τροποποίηση της ροής των μηνυμάτων και την άρνηση της υπηρεσίας. Απ' την άλλη, μια υπηρεσία ακεραιότητας χωρίς σύνδεση, που εξετάζει μεμονωμένα μηνύματα αδιαφορώντας για οτιδήποτε άλλο, παρέχει γενικά μόνο την προστασία ενάντια στην τροποποίηση των μηνυμάτων.

Μπορούμε να κάνουμε μια διάκριση μεταξύ της υπηρεσίας με και χωρίς αποκατάσταση. Επειδή η υπηρεσία ακεραιότητας αφορά τις ενεργές επιθέσεις, ενδιαφερόμαστε για την ανίχνευση παρά την πρόληψη. Εάν μια παραβίαση της ακεραιότητας ανιχνεύεται, τότε η υπηρεσία μπορεί απλά να εκθέσει αυτήν την παραβίαση, και κάποιο μέρος του λογισμικού ή ανθρώπινης επέμβασης απαιτείται για να ανακτήσει από την παραβίαση. Εναλλακτικά, υπάρχουν μηχανισμοί διαθέσιμοι για να ανακτήσουν από την απώλεια ακεραιότητας των δεδομένων. Η ενσωμάτωση των αυτοματοποιημένων μηχανισμών αποκατάστασης είναι, γενικά, πιο ελκυστική εναλλακτική λύση.

Μη απάρνηση

Η μη απάρνηση αποτρέπει είτε τον αποστολέα είτε το δέκτη από την άρνηση ενός μεταδιδόμενου μηνύματος. Κατά συνέπεια, όταν στέλνεται ένα μήνυμα, ο δέκτης μπορεί να αποδείξει ότι το μήνυμα εστάλη πράγματι από τον υποτιθέμενο αποστολέα. Ομοίως, όταν παραλαμβάνεται ένα μήνυμα, ο αποστολέας μπορεί να αποδείξει ότι το μήνυμα παραλήφθηκε πράγματι από τον υποτιθέμενο δέκτη.

Έλεγχος πρόσβασης

Στα πλαίσια της ασφάλειας δικτύων, ο έλεγχος πρόσβασης είναι η δυνατότητα να περιοριστεί και να ελεγχθεί η πρόσβαση στα συστήματα των χρηστών και τις εφαρμογές μέσω των συνδέσεων επικοινωνιών. Για να επιτευχθεί αυτός ο έλεγχος, κάθε οντότητα που προσπαθεί να αποκτήσει πρόσβαση πρέπει πρώτα να προσδιοριστεί ή να πιστοποιηθεί, έτσι ώστε τα δικαιώματα πρόσβασης να μπορούν να προσαρμοστούν στο άτομο.

Διαθεσιμότητα

Ποικίλες επιθέσεις μπορούν να οδηγήσουν στην απώλεια ή τη μείωση της διαθεσιμότητας. Μερικές από αυτές τις επιθέσεις υπάγονται στα αυτοματοποιημένα αντίμετρα, όπως η επικύρωση και η κρυπτογράφηση, ενώ άλλες απαιτούν κάποιο είδος φυσικής δράσης για να αποτρέψουν ή να ανακτήσουν από την απώλεια διαθεσιμότητας των στοιχείων ενός διανεμημένου συστήματος.

2.2 ΑΠΕΙΛΕΣ

Οι απειλές διακρίνονται σε τρεις βασικές κατηγορίες ανάλογα με το αίτιο εμφάνισης τους: *«Φυσικές απειλές»* που αναφέρονται σε φυσικά και περιβαλλοντολογικά φαινόμενα, *«απειλές απροσδόκητες ή αθέλητες»* **(accidental threats)** οι οποίες μπορούν να προκαλέσουν είτε την αποκάλυψη εμπιστευτικών πληροφοριών ή να δημιουργήσουν μια μη αποδεκτή κατάσταση στο σύστημα και *«σκόπιμες ή ηθελημένες»* **(intentional threats)** όπως οι *«προσβολές ή επιθέσεις»* **(attacks)** από εξωγενείς παράγοντες.

Φυσικές απειλές

Οι απειλές αυτού του είδους αναφέρονται κυρίως σε φυσικά φαινόμενα και άρα δεν είναι δυνατόν πάντα να αποτραπούν. Από την άλλη όμως είναι σημαντικό να αποφεύγονται ενέργειες που αυξάνουν την πιθανότητα εκδήλωσης τους (π.χ. κάπνισμα σε «κρίσιμους» χώρους. Ωστόσο, η ύπαρξη έτοιμου εφεδρικού συστήματος (back-up system) με την ανάλογη

λήψη εφεδρικών αρχείων για τα κρίσιμα δεδομένα του συστήματος, μπορεί να περιορίσει τις κακές συνέπειες από την εκδήλωση τέτοιων απειλών.

Απροσδόκητες απειλές

Οι απροσδόκητες απειλές μπορούν να εξελιχθούν σε κινδύνους που έχουν σχέση με την αποκάλυψη ή την τροποποίηση αντικειμένων (κυρίως πληροφοριών). Τέτοιου είδους *«αποκάλυψη»* μπορεί να προκληθεί από αστοχία στο υλικό του συστήματος ή στις εφαρμογές και τα προγράμματα που εκτελούνται σε αυτό αλλά και από τους χρήστες καθώς και από λάθη χειρισμών. Αποτέλεσμα αυτών των απειλών είναι η απώλεια εμπιστευτικότητας. Για παράδειγμα ένας χρήστης, ο οποίος από λάθος χειρισμό στέλνει μέσω ηλεκτρονικού ταχυδρομείου ένα εμπιστευτικό μήνυμα σε λάθος παραλήπτη, αποτελεί απροσδόκητη ή αθέλητη απειλή για την ασφάλεια του συστήματος.

Μια απροσδόκητη απειλή μπορεί να προκαλέσει ακόμη και την τροποποίηση ενός αντικειμένου η οποία μπορεί να θεωρηθεί ως παραβίαση της ακεραιότητας του. Ως αντικείμενο μπορεί να θεωρηθεί είτε μια πληροφορία ή ακόμη και κάποιος πόρος του συστήματος.

Απειλές από επιθέσεις (εισβολές στο σύστημα)

Μια εισβολή στο σύστημα αποτελεί απειλή που προκαλείται σκόπιμα και πραγματοποιείται από οντότητες που έχουν σκοπό την παραβίαση της ασφάλειας. Οι εισβολές συνήθως έχουν σαν στόχο την καταστροφή, την υποκλοπή ή την τροποποίηση πληροφοριών. Με αυτό τον τρόπο αποκαλύπτονται πληροφορίες οπότε έχουμε απώλεια εμπιστευτικότητας ή τροποποιούνται άρα έχουμε παραβίαση της ακεραιότητας των πληροφοριών.

Οποιαδήποτε προσπάθεια η οποία καταστρατηγεί τους κανόνες ασφάλειας, όπως αυτοί έχουν καθοριστεί μέσω της πολιτικής ασφάλειας, η οποία με τη σειρά της προσδιορίζει τους επιτρεπτούς τρόπους πρόσβασης στα αντικείμενα του συστήματος, θεωρείται ως παραβίαση των κανόνων ασφάλειας.

2.2.1 ΕΠΙΘΕΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Οι επιθέσεις στην ασφάλεια ενός συγκροτήματος ηλεκτρονικών υπολογιστών ή ενός δικτύου χαρακτηρίζονται καλύτερα από την εξέταση της λειτουργίας του συγκροτήματος ηλεκτρονικών υπολογιστών ως προς την παροχή πληροφοριών. Γενικά, υπάρχει μια ροή των πληροφοριών από μια πηγή, όπως ένα αρχείο ή μια περιοχή της κύριας μνήμης, προς έναν προορισμό, όπως ένα άλλο αρχείο ή ένας χρήστης.

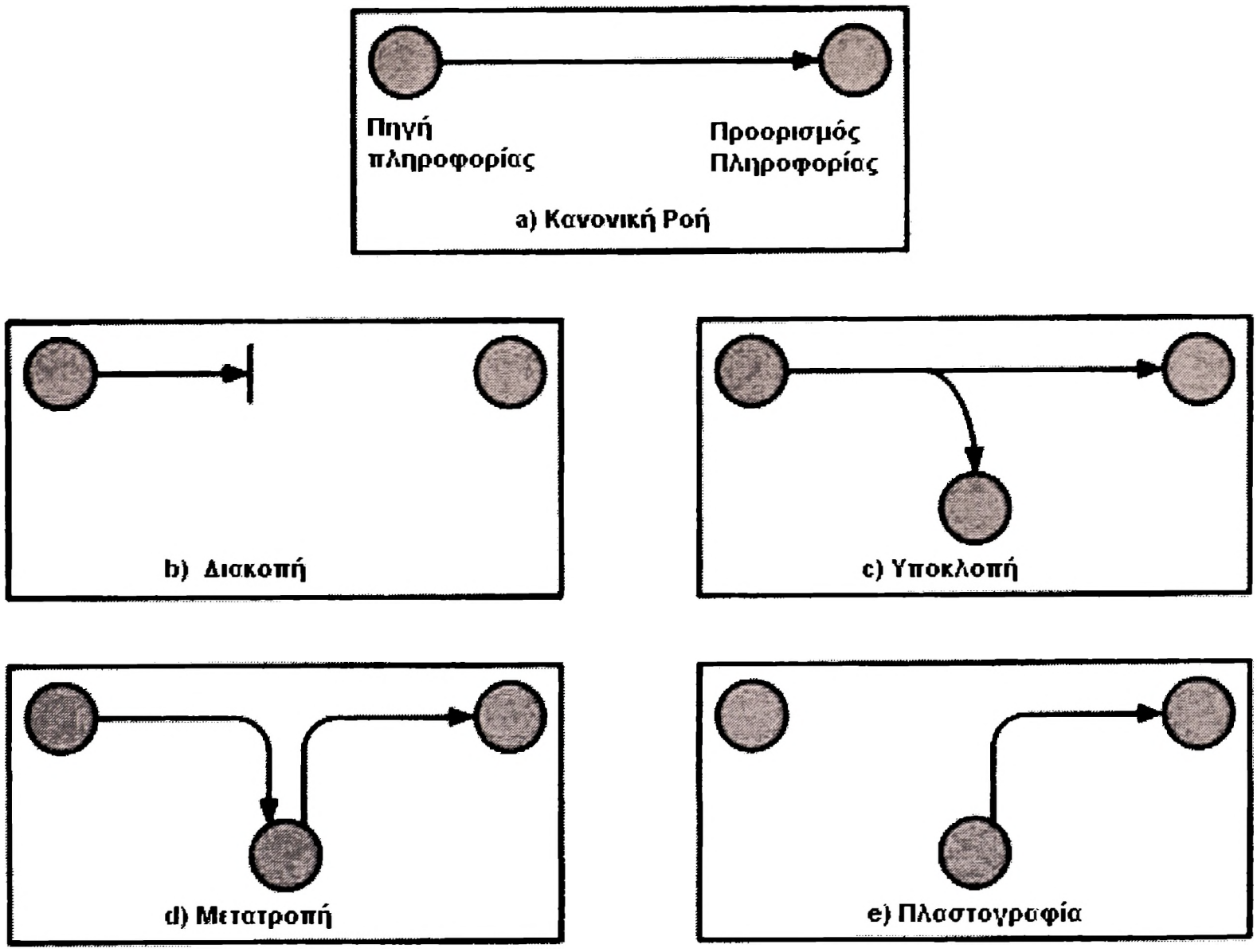
Αυτή η κανονική ροή απεικονίζεται στο σχήμα 2-1a.

Τα υπόλοιπα μέρη του σχήματος παρουσιάζουν τις ακόλουθες τέσσερις γενικές κατηγορίες επίθεσης [Stall99]:

- ***Διακοπή (interruption)***: Ένα μέρος του συστήματος γίνεται μη διαθέσιμο ή άχρηστο ή χάνεται εντελώς. Σε αυτή την περίπτωση έχουμε άρνηση εξυπηρέτησης (denial of service) του συστήματος προς τους εξουσιοδοτημένους χρήστες του.
- ***Υποκλοπή (interception)***: Κάποιο μη εξουσιοδοτημένο άτομο έχει καταφέρει να αποκτήσει προσπέλαση σε ένα τμήμα του συστήματος (π.χ. κλοπή εξαρτημάτων,

παρακολούθηση δεδομένων στο δίκτυο, κλπ.). Σε αυτή την περίπτωση παραβιάζεται η εμπιστευτικότητα των δεδομένων του συστήματος.

- ***Μετατροπή (modification)***: Κάποιο μη εξουσιοδοτημένο άτομο αποκτά πρόσβαση σε μέρος του συστήματος και παραποιεί λογισμικό ή πληροφορίες (δεδομένα) του συστήματος. Πρόκειται κυρίως για παραβίαση της ακεραιότητας του συστήματος.
- ***Πλαστογραφία (fabrication)***: Είναι απειλή που αναφέρεται αποκλειστικά στα δεδομένα του συστήματος και συμβαίνει όταν ένα μη εξουσιοδοτημένο άτομο εισάγει επιπλέον - παραποιημένα δεδομένα σε ένα σύστημα. Πρόκειται για απειλή κατά της ακεραιότητας και της διαθεσιμότητας του συστήματος.



Σχήμα 2-1: ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ

Μια χρήσιμη κατηγοριοποίηση των παραπάνω επιθέσεων είναι σε ***παθητικές*** και ***ενεργητικές*** επιθέσεις.

Παθητικές (passive). Θεωρούνται αυτές που έχουν σαν στόχο την παρακολούθηση ενός συστήματος και τη συλλογή πληροφοριών για τον τρόπο λειτουργίας του. Γενικά είναι δύσκολο να εντοπισθεί μια παθητική εισβολή διότι συνήθως δεν απαιτεί αλληλεπίδραση με το σύστημα και δεν διαταράσσει την ομαλή λειτουργία του. Ως παράδειγμα μπορεί να θεωρηθεί η παρακολούθηση κυκλοφορίας σε ένα δίκτυο δεδομένων. Η κρυπτογράφηση

μπορεί να λύσει μερικώς το πρόβλημα διότι η ύπαρξη και μόνο κίνησης σε ένα δίκτυο μπορεί να προκαλέσει αποκάλυψη πληροφοριών αναλύοντας για παράδειγμα χρόνους και συχνότητες μετάδοσης ή μήκος πληροφορίας ανεξάρτητα από περιεχόμενο.

Ενεργητικές (active). Θεωρούνται αυτές που προκαλούν αλλαγές στη συμπεριφορά ενός συστήματος. Για παράδειγμα η παρεμβολή μηνυμάτων σε ένα δίκτυο, η πρόκληση καθυστέρησης, η αναδιάταξή τους, η αναπαραγωγή ή και η διαγραφή υπαρχόντων μηνυμάτων, η σκόπιμη εκμετάλλευση του λογισμικού του συστήματος για την πρόκληση ζημιάς κλπ. Μια απλή ενέργεια όπως αυτή της τροποποίησης μιας αρνητικής αναγνώρισης (NACK) από ένα εξυπηρετητή δεδομένων (database server) σε θετική (ACK), μπορεί να προκαλέσει μεγάλη σύγχυση ή και ζημιά. Οι ενεργητικές επιθέσεις σε αντίθεση με τις παθητικές μπορούν να εντοπιστούν ευκολότερα αν έχουν ληφθεί τα κατάλληλα μέτρα.

2.2.2 ΕΡΓΑΛΕΙΑ ΕΠΙΘΕΣΗΣ

2.2.2.1 ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ (TROJAN HORSES)

Οι Δούρειοι Ίπποι (Trojan horses) είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Συνήθως κρύβονται σε άλλα προγράμματα, αλλά μπορούν να βρίσκονται και μεμονωμένα. Παράδειγμα Δούρειου Ίππου είναι ο Happy99.exe [Site2]. Αυτοί αντιπροσωπεύουν ποσοστό 58% του συνόλου των εργαλείων επίθεσης.

2.2.2.2 «ΣΚΟΥΛΗΚΙΑ» (WORMS)

Τα σκουλήκια είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα, αλλά συνήθως δεν προκαλούν άλλου τύπου επιπλοκές. Τα σκουλήκια μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα που μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων. Για τη δημιουργία απαιτούνται ειδικές γνώσεις πρωτοκόλλων επικοινωνιών, ευπαθειών δικτυακών συστημάτων και ειδικών θεμάτων πάνω σε λειτουργικά συστήματα.

Τα σκουλήκια μπορούν να εκτελούν και κακόβουλες πράξεις που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης. Αυτό συνήθως προκαλείται από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα.

2.2.2.3 ΙΟΙ (VIRUSES)

Οι Ιοί (viruses), τα γνωστά προγράμματα που προσπαθούν (με πονηρές και συνήθως δόλιες τεχνικές) να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μία υπογραφή-ίχνος της παρουσίας τους, μέχρι πιο επώδυνους, απώλεια δεδομένων, καταστροφή της διαμόρφωσης (configuration) του συστήματος, κλπ.).

Όσον αφορά τον τρόπο ενεργοποίησής τους, οι ιοί αντιγράφονται από μόνοι τους με δύο βασικούς τρόπους. Όταν εκτελείται ένα μολυσμένο πρόγραμμα:

- είτε μολύνει άμεσα άλλα μέρη του υπολογιστή, π.χ άλλες τοποθεσίες στο δίσκο ή άλλα προγράμματα
- είτε εγκαθίσταται μόνιμα στη μνήμη από μόνο του και κατόπιν μολύνει άλλα προγράμματα που εκτελούνται ή μέσα αποθήκευσης που εισάγονται για χρήση (π.χ. δισκέτες).

Οι ιοί που εισχωρούν σε ένα σύστημα δεν μπορούν να παραμείνουν ολότελα αόρατοι αφού ο ιοικός κώδικας πρέπει να αποθηκευτεί κάπου. Παρόλα αυτά οι ιοί μπορούν να κρύβονται (κατά ένα μέρος) είτε τεμαχίζοντας τον κώδικα τους είτε αποθηκευόμενοι σε κρυπτογραφημένη μορφή, όπως οι πολυμορφικοί ιοί, χρησιμοποιώντας ένα μεταβλητό κρυπτογραφικό κλειδί το οποίο επίσης αποθηκεύεται μαζί με τον κρυπτογραφημένο ιοικό κώδικα. Όμως, το μέρος του ιοικού κώδικα που είναι υπεύθυνο για την διαδικασία αποκρυπτογράφησης πρέπει να παραμείνει χωρίς κρυπτογράφηση, αφήνοντας έτσι μια υπογραφή που είναι ικανή για τον εντοπισμό των ιών αυτών.

2.2.2.4 «ΑΝΙΧΝΕΥΤΕΣ» (SCANNERS)

Οι ανιχνευτές (scanners) δικτυακής κίνησης είναι προγράμματα που χρησιμοποιούνται για τον έλεγχο της ασφάλειας των συστημάτων. Ονομάζονται ανιχνευτές γιατί γνωρίζουν όλα τα πιθανά εξωτερικά σημεία που θα μπορούσε να εκμεταλλευτεί ένας επίδοξος hacker για να προσβάλει την ασφάλεια του συστήματος. Αν και αρχικά δημιουργήθηκαν για χρήση από τους διαχειριστές των συστημάτων, σύντομα έγιναν εργαλεία των hackers για να βρίσκουν πιθανούς στόχους. Το ποσοστό της χρήσης τους είναι 14.3% του συνόλου των εργαλείων επίθεσης.

2.2.2.5 «ΣΠΑΣΤΗΡΙΑ ΚΩΔΙΚΩΝ» (PASSWORD CRACKS)

Τα «σπαστήρια κωδικών» (password cracks) είναι προγράμματα τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης (password file) και με χρήση ενός Λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται ως κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Ενδεικτικά αναφέρεται ότι σε ένα UNIX σύστημα 1000 περίπου χρηστών, και υποθέτοντας ότι οι χρήστες δεν έχουν συμβουλευτεί να επιλέγουν δύσκολους κωδικούς (συνήθως συνδυασμό γραμμάτων, αριθμών και σημείων στίξης), ένα «σπαστήρι» μπορεί να ανακαλύψει εύκολα ένα ποσοστό 40% των

συνολικών κωδικών. Τα προγράμματα αυτά χρησιμοποιούν και οι διαχειριστές συστημάτων για να προλάβουν παρόμοιες ενέργειες από hackers.

2.2.2.6 «ΩΤΑΚΟΥΣΤΕΣ» ΠΑΚΕΤΩΝ (PACKET SNIFFERS)

Οι «Ωτακουστές» πακέτων (packet sniffers) είναι προγράμματα που μπορούν να παρακολουθούν («ακούν», ή «μυρίζουν» - sniff) την κίνηση του δικτύου σε επίπεδο IP πακέτων. Με κατάλληλες τεχνικές, έχουν την δυνατότητα να ανακατασκευάσουν τα μηνύματα και να κάνουν αναγνώριση των πρωτοκόλλων που περνούν πάνω από το δίκτυο. Οι «Ωτακουστές» τρέχουν συνήθως σε τοπικά δίκτυα (Ethernet) και «κλέβουν» κωδικούς πρόσβασης ή παρακολουθούν τις πληκτρολογήσεις από συγκεκριμένους σταθμούς εργασίας. Με κατάλληλους μηχανισμούς ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμη πληροφορία (κωδικούς πρόσβασης, αρχεία, κλπ.) χωρίς όμως να επηρεάζουν το περιεχόμενό τους (ανάγνωση μόνο). Τα γεγονότα που αφορούν «Ωτακουστές» ανταποκρίνονται σε ένα ποσοστό 31% του συνόλου των εργαλείων επίθεσης.

Ο τρόπος επίθεσης με αυτούς εφαρμόζει μία κλιμάκωση στον τρόπο δράσης: ξεκινά από απλή ανίχνευση του στόχου κι αφού εντοπίσει παραλείψεις στην ασφάλεια, εισβάλλει, σβήνει τα ίχνη, αποδυναμώνει την άμυνα του συστήματος (π.χ τη Δικτυακή Υπηρεσία Πληροφοριών - NIS, το Πρωτόκολλο Μεταφοράς Αρχείων – FTP κλπ) και εγκαθιστά Trojans για την εξάπλωση του.

Η χρήση των «Ωτακουστών» αν και μπορεί να έχει θετικά αποτελέσματα για την διαχείριση δικτύου και υπολογιστικών συστημάτων (εντοπισμός bottlenecks, άχρηστης πληροφορίας που μεταδίδεται κλπ.) στα χέρια των hackers μπορεί να έχει καταστροφικά αποτελέσματα. Η χρήση ενός «Ωτακουστή» απαιτεί προνόμια διαχειριστή (superuser privileges), αλλά σήμερα, ο καθένας είναι «διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο. Για τον λόγο αυτό, η ασφάλεια από τα sniffers θα πρέπει να εξασφαλίζεται στο επίπεδο Παρόχου Υπηρεσιών Διαδικτύου (Internet Service Provider – ISP).

2.2.2.7 «ΜΟΧΘΗΡΟΣ ΚΩΔΙΚΑΣ» (MALICIOUS CODE)

Πρόκειται για εντολές οι οποίες δείχνουν να ξεκινούν διαδικασίες χρηστών, αλλά στην πραγματικότητα προσπαθούν να μαζέψουν ή να εκμεταλλευτούν ευαίσθητα δεδομένα (password files). Για παράδειγμα στην κατηγορία αυτή μπορούν να ενταχθούν οι προσπάθειες για σύνδεση μέσω του προγράμματος login, μέσω συνδέσεων http και telnet.

2.3 ΤΑ ΒΑΣΙΚΟΤΕΡΑ ΕΙΔΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΔΙΚΤΥΩΝ

- ***Υποκλοπή επικοινωνιών.*** Οι ηλεκτρονικές επικοινωνίες μπορούν να υποκλαπούν και τα δεδομένα να αντιγραφούν ή να τροποποιηθούν [Site3]. Η υποκλοπή μπορεί να πραγματοποιηθεί με διάφορους τρόπους.

Ενδεχόμενη ζημία: Η παράνομη υποκλοπή μπορεί να προξενήσει βλάβη, τόσο ως παραβίαση της ιδιωτικής ζωής των ατόμων, όσο και μέσω της εκμετάλλευσης των δεδομένων που έχουν υποκλαπεί, όπως συνθηματικών ή στοιχείων από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά.

- ***Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών (hacking, cracking).*** Η μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή ή σε ένα δίκτυο υπολογιστών πραγματοποιείται συνήθως κακόβουλα με την πρόθεση αντιγραφής, τροποποίησης ή καταστροφής δεδομένων. Αυτό τεχνικά αποκαλείται παρείσφρηση και μπορεί να γίνει με διάφορους τρόπους, όπως: i) με την αξιοποίηση πληροφοριών που προέρχονται από το εσωτερικό, επιθέσεις «λεξικού», ii) με βίαιες επιθέσεις (εκμεταλλευόμενες την τάση των χρηστών να επιλέγουν προβλέψιμα συνθηματικά), iii) με χειραγώγηση (που εκμεταλλεύεται την τάση των χρηστών να αποκαλύπτουν πληροφορίες σε φαινομενικά αξιόπιστα άτομα), και iv) με την υποκλοπή συνθηματικών.

  Ενδεχόμενη ζημία: Η μη εξουσιοδοτημένη παρείσφρηση έχει ενίοτε ως κίνητρο διανοητική πρόκληση και όχι κερδοσκοπία. Ωστόσο, αυτό που αρχίζει ως μια διαδικασία παρενόχλησης αναδεικνύει τα τρωτά σημεία των δικτύων πληροφοριών και παρακινεί άτομα με εγκληματική ή δόλια πρόθεση να εκμεταλλευθούν αυτές τις αδυναμίες. Η προστασία κατά της μη εξουσιοδοτημένης πρόσβασης σε προσωπικές πληροφορίες, περιλαμβανομένων οικονομικών πληροφοριών, τραπεζικών λογαριασμών και δεδομένων υγείας, αποτελεί δικαίωμα των ατόμων. Για το δημόσιο τομέα και τη βιομηχανία, οι επιβουλές κυμαίνονται από την οικονομική κατασκοπεία έως τη δυνητική τροποποίηση εσωτερικών ή δημόσιων δεδομένων, συμπεριλαμβανομένης της αλλοίωσης του περιεχομένου δικτυακών τόπων.

- ***Διατάραξη δικτύων (denial of service), δηλαδή πρόκληση κατάρρευσης ενός δικτύου λόγω υπερφόρτωσης.*** Τα δίκτυα είναι σε μεγάλο βαθμό ψηφιοποιημένα και ελέγχονται από υπολογιστές. Ο πλέον κοινός λόγος διατάραξης δικτύου υπήρξε κατά το παρελθόν η βλάβη στο σύστημα υπολογιστή που ελέγχει το δίκτυο, ενώ οι επιθέσεις εναντίον δικτύου κατευθύνονταν κυρίως προς τους εν λόγω υπολογιστές. Σήμερα, οι περισσότερες επιθέσεις εκμεταλλεύονται τις αδυναμίες και ευπάθειες των συστατικών στοιχείων του δικτύου (λειτουργικά συστήματα, δρομολογητές, μεταγωγείς, εξυπηρετητές ονομάτων κλπ.).

  Οι επιθέσεις μπορούν να λάβουν διάφορες μορφές: α) Επιθέσεις εναντίον εξυπηρετητών ονομάτων τομέα (Domain Name Service – DNS), β) Επιθέσεις δρομολόγησης, γ) Επιθέσεις άρνησης παροχής υπηρεσίας.

  Ενδεχόμενη ζημία: Οι διακοπές είναι επιζήμιες για ορισμένες ιστοσελίδες, καθώς οι επιχειρήσεις βασίζονται ολοένα περισσότερο στην ανεμπόδιστη διάθεση των δικτυακών τους τόπων για τις εμπορικές τους συναλλαγές.

- ***Εκτέλεση κακόβουλου λογισμικού που τροποποιεί ή καταστρέφει δεδομένα (ιοί, worms και Trojan horses).*** Οι υπολογιστές λειτουργούν με λογισμικό. Το λογισμικό όμως μπορεί επίσης να χρησιμοποιηθεί και για να θέσει εκτός λειτουργίας έναν υπολογιστή, για να εξαλείψει ή

να τροποποιήσει δεδομένα. Εάν ένας τέτοιος υπολογιστής είναι μέρος του δικτύου διαχείρισης, μπορεί η δυσλειτουργία του να έχει εκτεταμένες επιπτώσεις. Ο ιός είναι μια μορφή κακόβουλου λογισμικού. Πρόκειται για ένα πρόγραμμα που αναπαράγει τον κώδικά του, προσκολλώμενο σε άλλα προγράμματα, με τρόπο ώστε ο κώδικας του ιού να εκτελείται κατά την εκτέλεση προγράμματος του υπολογιστή που έχει προσβληθεί. Υπάρχουν πολλοί άλλοι τύποι κακόβουλου λογισμικού. Ορισμένοι βλάπτουν μόνο τον υπολογιστή όπου έχουν αντιγραφεί, ενώ άλλοι μεταδίδονται σε άλλα δικτυωμένα προγράμματα. Υπάρχουν π.χ προγράμματα (με την ονομασία «λογικές βόμβες») που παραμένουν αδρανή μέχρι την ενεργοποίησή τους από κάποιο γεγονός, όπως μια συγκεκριμένη ημερομηνία, π.χ. Τρίτη και 13. Άλλα προγράμματα εμφανίζονται ως καλοήθη, όταν όμως ανοίγουν εκδηλώνουν κακόβουλη επίθεση (για το λόγο αυτό αποκαλούνται «Δούρειοι Ίπποι» - Trojans). Άλλα προγράμματα (ονομαζόμενα «Σκουλήκια» - Worms) δεν προσβάλλουν άλλα προγράμματα όπως ο ιός, αλλά δημιουργούν αντίγραφά τους, τα οποία με τη σειρά τους αναπαράγονται, κατακλύζοντας τελικά ολόκληρο το σύστημα.

Ενδεχόμενη ζημία: Οι ιοί μπορούν να είναι ιδιαίτερα καταστροφικοί, όπως φαίνεται και από το υψηλό κόστος ορισμένων πρόσφατων επιθέσεων (π.χ. "I Love you", "Melissa" και "Kournikova").

- ***Παραπλάνηση/ψευδής δήλωση.*** Με την αποκατάσταση μιας δικτυακής σύνδεσης ή την παραλαβή δεδομένων, ο χρήστης συνάγει την ταυτότητα του συνομιλητή του με βάση το περικείμενο (context) της επικοινωνίας. Το δίκτυο παρέχει ορισμένες ενδείξεις ως προς αυτό. Ωστόσο, ο μεγαλύτερος κίνδυνος επιθέσεων προέρχεται από άτομα που γνωρίζουν το περικείμενο «από μέσα», δηλ. από μυημένους. Όταν ένας χρήστης επιλέγει έναν αριθμό ή έναν τύπο ηλεκτρονικής διεύθυνσης στον υπολογιστή, αναμένει ότι θα φθάσει στον επιθυμητό προορισμό. Αυτό αρκεί για πολλές εφαρμογές, όχι όμως για σημαντικές επαγγελματικές συναλλαγές ή για ιατρικές, οικονομικές ή επίσημες επικοινωνίες, όπου απαιτείται υψηλότερος βαθμός ελέγχου ταυτότητας, ακεραιότητας και τήρησης του απορρήτου.

  Ενδεχόμενη ζημία: Η παραπλάνηση ατόμων ή φορέων είναι επιζήμια κατά διαφορετικούς τρόπους. Οι πελάτες ενδέχεται να τηλε-φορτώσουν κακόβουλο λογισμικό από δικτυακό τόπο που αντιποιείται έμπιστη πηγή. Ενδέχεται να δοθούν εμπιστευτικές πληροφορίες σε λάθος άτομα. Η παραπλάνηση είναι δυνατόν να οδηγήσει σε άρνηση αναγνώρισης online συμβάσεων κλπ. Η μεγαλύτερη ίσως ζημία είναι το γεγονός ότι η έλλειψη επαλήθευσης ταυτότητας αποτρέπει δυνητική πελατεία.

2.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΠΙΘΕΣΕΩΝ ΠΟΥ ΕΧΟΥΝ ΣΥΜΒΕΙ ΔΙΕΘΝΩΣ

2.4.1 ΟΙ ΟΛΛΑΝΔΟΙ HACKERS (DUTCH HACKERS)

Η ιστορία των Ολλανδών hackers είναι το πιο μεγάλο σε διάρκεια περιστατικό, όπως καταγράφεται στο CERT®/CC [Site4]. Ξεκίνησε την 1η Απριλίου 1990 με την προσπάθεια

εισβολής σε μηχανήματα του domain .mil (Αμερικανικός Στρατός). Η διάρκεια του ήταν σχεδόν δύο χρόνια και αναφέρθηκαν ως προσβεβλημένα 383 sites σε όλο τον κόσμο (ένα και στην Ελλάδα). Η ιστορία αυτή εξελίχθηκε παράλληλα με τον Πόλεμο του Κόλπου και κάποιες προεκτάσεις του θα μπορούσαν να δημιουργήσουν σημαντικά προβλήματα στην αποστολή.

Οι hackers κατάφεραν και εισέβαλαν σε 34 αμερικάνικους στρατιωτικούς ιστότοπους στο διαδίκτυο, συμπεριλαμβανομένων και ιστότοπων που συμμετείχαν στην υποστήριξη της επιχείρησης «Desert Storm/Shield». Έψαξαν αρχεία και ηλεκτρονικό ταχυδρομείο για την αναζήτηση λέξεων όπως «πυρηνικά», «όπλα», «πύραυλοι», «desert shield», «desert storm». Βρήκαν πληροφορίες για την ακριβή θέση των αμερικανικών στρατευμάτων, τον τύπο των όπλων που είχαν, τις δυνατότητες των πυραύλων Patriot και τις κινήσεις των αμερικανικών πλοίων στον Κόλπο. Όταν μάζεψαν τις πληροφορίες έσβησαν τα ίχνη τους.

Σύμφωνα με τον Jim Christy, έναν από τους υπεύθυνους του προγράμματος για την ανακάλυψη εγκλημάτων πληροφοριών σε θέματα πολέμου, του γραφείου της Αμερικάνικης αεροπορίας (Air Force Office of Special Investigations), οι επιθέσεις αφορούσαν και συστήματα τροφοδοσίας των στρατευμάτων στον Κόλπο. «Θα μπορούσαν αντί για πυρομαχικά να είχαν στείλει οδοντόβουρτσες», είπε χαρακτηριστικά στο ABCNews.

Οι hackers είχαν τόση πληροφορία που γέμισαν τους δίσκους τους, τις δισκέτες, και φύλαξαν μέρος της λείας τους σε χώρο των υπολογιστικών συστημάτων στο Bowling Green University και στο University of Chicago. Κατά πληροφορίες, οι εισβολείς επιχείρησαν να πουλήσουν πληροφορίες στο Ιράκ κατά την διάρκεια του πολέμου. Η πληροφορία μεταδόθηκε από το BBC, που είχε την πληροφορία από κυβερνητικούς αξιωματούχους στο Ιράκ, αλλά ο Σαντάμ Χουσεΐν αρνήθηκε την προσφορά του ενδιάμεσου των hackers, γιατί φοβήθηκε παγίδα.

Ακόμα και όταν οι εισβολείς εντοπίστηκαν δεν μπορούσαν να τους συλλάβουν γιατί εκείνο τον καιρό οι επιθέσεις σε υπολογιστές δεν ήταν παράνομες. Το FBI προσπάθησε να φέρει τον κύριο εμπνευστή της ομάδας των εισβολέων στην Αμερική, για μία συνέντευξη για δουλειά από μεγάλη αεροναυπηγική εταιρία στην Florida. Όμως αυτός ειδοποιήθηκε κατα λάθος και το κατάλαβε. Τελικά δύο από τους εισβολείς συλλαμβάνονται και οδηγούνται στην φυλακή για παραποίηση στοιχείων και χρήση πιστωτικής κάρτας.

Οι Ολλανδοί hackers χρησιμοποίησαν διάφορες μεθόδους προκειμένου να πετύχουν τους σκοπούς τους. Για τον λόγο αυτό αναφέρονται οι Μέθοδοι Δράσης του CERT®/CC με τις οποίες συσχετίστηκαν: weak passwords, no passwords, password files, password cracking, Trojan login, FTP, deleted files, open servers, social engineering, user accounts, system accounts, login attempts, hosts.equiv, .rhosts, sendmail attacks, debug, chsh/chfn, mail spoofing, rm -rf /, 87 socket, software piracy.

Όλα τα παραπάνω τα κατάφεραν, είτε χρησιμοποιώντας απλές εντολές που έδιναν με το χέρι, είτε με χρήση απλών προγραμμάτων (scripts). Ιδιαίτερο ενδιαφέρον παρουσιάζει η αναφορά στο «socket 87» που ήταν η «πίσω πόρτα» για να επανέρχονται σε συστήματα που είχαν ήδη χτυπήσει.

Η επίθεση των Ολλανδών hackers, απέδειξε την αδυναμία των ιστότοπων να θωρακιστούν απέναντι σε μία απειλή που συνεχώς άλλαζε πρόσωπο και τρόπους δράσης. Είναι αμφίβολο αν η δράση τους θα σταματούσε στις αρχές του 1992 αν δεν είχε επέμβει η Ολλανδική Αστυνομία. Σε κάθε περίπτωση, η επίθεση αυτή θα μείνει ως η πιο μεγάλη σε διάρκεια (712 μέρες) και σφοδρότητα (για την εποχή της).

2.4.2 ΟΙ ΔΑΝΟΙ HACKERS

Είναι μία παρόμοια επίθεση με αυτή των Ολλανδών hackers, αυτή τη φορά όμως από την Δανία. Είχε διάρκεια από τον Αύγουστο του 1993 ως και τον Δεκέμβριο του ίδιου έτους (οπότε και επενέβη η Δανική Αστυνομία).

Τα χαρακτηριστικά της επίθεσης, με βάση τους τρόπους δράσης που καταγράφηκαν στο CERT®/CC είναι τα εξής: sendmail, ISS attack, password files, password cracking, files deleted, mail spoofing, Trojan horses.

Όπως φαίνεται, η δράση τους αποτελεί ένα μικρό υποσύνολο της δράσης των Ολλανδών hackers. Ένα νέο χαρακτηριστικό της επίθεσης ήταν η χρήση του εργαλείου ISS (Internet Security Scanner), το οποίο μπορεί και ανιχνεύει για παραλείψεις στην ασφάλεια των συστημάτων ενός υποδικτύου. Αν και αρχικά προοριζόταν για χρήση από τους διαχειριστές συστημάτων, σύντομα ξέφυγε από το έλεγχο κι έγινε όπλο στις επιθέσεις των hackers.

Η επίθεση των Δανών hackers, το δεύτερο εξάμηνο το 1993, είχε ως στόχο και 2 Ελληνικά sites.

2.4.3 ΕΠΙΘΕΣΗ ΜΕΣΩ ΤΟΥ IRC

Το IRC (Internet Relay Chat) αποτελεί τον κυριότερο και παλιότερο τρόπο επικοινωνίας των χρηστών του Internet. Σε διάφορους χώρους (κανάλια, όπως ονομάζονται στην ορολογία του IRC) μπορεί κανείς να μπει και να δει συζητήσεις σε θέματα διάφορων ενδιαφερόντων (από πολιτική μέχρι hacking).

Το «Περιστατικό #18» του CERT®/CC αφορά σε επιθέσεις μέσω του IRC. Χρησιμοποιώντας μεθόδους social engineering, hackers έπειθαν τους απλούς και αφελείς χρήστες να εκτελούν εντολές (τις λεγόμενες DCC εντολές) ώστε να αποκτούν πρόσβαση στο λογαριασμό τους. Στην συνέχεια, με χρήση κλασικών μεθόδων συνέχιζαν τις επιθέσεις τους. Η πιο χαρακτηριστική περίπτωση ήταν να πείθουν αρχάριους χρήστες να τρέξουν την εντολή "rm -rf / &" από το λογαριασμό τους, με τα γνωστά καταστροφικά αποτελέσματα.

Ένα επίσης σοβαρό περιστατικό, το «Περιστατικό #16», έχει καταγραφεί ως ένα από τα σφοδρότερα στα αρχεία του CERTO/CC. Η διάρκεια του ήταν 224 μέρες (μέσα 1994-μέσα 1995) και χτυπήθηκαν 515 sites. Οι μέθοδοι δράσης που καταγράφηκαν αφορούσαν: rootkit, sniffer, user accounts, system accounts, crack, login attempts, NIS attack, rdist, social engineering, system files deleted, Trojan IRC, Trojan ls, Trojan ifconfig, Trojan ps, Trojan login, Trojan mail, weak password, password file, password cracking, TFTP attack, uudecode alias, sendmail attack, IRC abuse, IRC flooding, password -f, mail spoofing, mail bombs, DOS attack, guest account, no password, FTP abuse, software piracy, telnet connections, rlogin connections, mailrace, NFS attack, halt system, chain letter, lpr print, expreserve, SATAN, configuraton, gopher, httpd, uucp, rexd attack, warez, open servers.

Χαρακτηριστικά αναφέρεται ότι από τα 515 sites που χτυπήθηκαν σε όλον το κόσμο, 2 ήταν και στην Ελλάδα. Το περιστατικό αυτό παρουσιάζει για πρώτη φορά μία ευρεία γεωγραφική κατανομή στην επιλογή των στόχων (χτυπήθηκαν 41 top-level domains) .

2.4.4 ΚΛΟΠΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Το 2000 ήταν το έτος που έγιναν γνωστές αρκετές περιπτώσεις κλοπής απόρρητων

προσωπικών δεδομένων. Στην αρχή του χρόνου ένας δεκαοκτάχρονος Ρώσος με το ψευδώνυμο Maxus, εισέβαλε στο ηλεκτρονικό κατάστημα πώλησης μουσικής CDUniverse και έκλεψε τα στοιχεία των πελατών του. Όταν η εταιρία που εξυπηρετούσε ηλεκτρονικά (hosting) τις υπηρεσίες της CDUniverse αρνήθηκε να πληρώσει $100,000 σαν λύτρα στον κλέφτη, αυτός δημοσίευσε 25,000 πιστωτικές κάρτες στο διαδίκτυο, ενώ ισχυρίστηκε πως είχε άλλες 300,000.

Τον ΣεπτέμΒρη 2000 εκλάπησαν 15,700 πιστωτικές κάρτες από την Western Union. Η μητρική εταιρία First Data προσφέρει ένα δίκτυο ηλεκτρονικών οικονομικών συναλλαγών στο 75% του κόσμου παρέχοντας υπηρεσίες με πιστωτικές κάρτες σε 1,400 οργανισμούς και 343 εκατομμύρια καταναλωτές παγκοσμίως.

Στις αρχές του Δεκεμβρίου 2000, ένας κυβερνοκλέφτης από την Ρωσία, έκλεψε 55,000 πιστωτικές κάρτες από την CreditCards.com, μία εταιρία που επεξεργάζεται και επιβεβαιώνει την ακρίβεια των στοιχείων πιστωτικών καρτών για μικρομεσαίες επιχειρήσεις στο διαδίκτυο. Δύο μέρες αργότερα ένας άλλος εισέβαλε και έκλεψε τα ηλεκτρονικά αρχεία 5,000 ασθενών του Washington University Hospital, με το ιατρικό ιστορικό και τους αριθμούς κοινωνικής ασφάλισης τους.

2.4.5 ΑΠΟ ΤΙΣ ΦΙΛΙΠΠΙΝΕΣ, ΜΕ ΑΓΑΠΗ

Τον Μάιο του 2000, εμφανίστηκε ο ιός των ερωτικών γραμμάτων, γνωστός σαν ILOVEYOU [Site5]. Ο ιός αυτός είχε πολλά κοινά στοιχεία με τον Melissa [Site4a] και δημιούργησε αρκετά προβλήματα, αφήνοντας πίσω του χαλασμένα αρχεία και χάος. Το FBI ανίχνευσε και βρήκε πως ο ιός προερχόταν από τον Onel de Guzman, έναν 22χρονο μαθητή στα προάστια της Μανίλα στις Φιλιππίνες.

Αν και δεν υπήρχαν εθνικοί νόμοι για αυτού του είδους τα αδικήματα, βρήκαν τρόπο να τον καταδικάσουν για πλαστογραφία πιστωτικών καρτών. Μετά από αυτό το περιστατικό, σύμφωνα με μία μελέτη της McConnell International, οι Φιλιππίνες είναι το μοναδικό κράτος που έχει ολοκληρωμένη κάλυψη για 10 διαφορετικές κρίσιμες περιοχές ηλεκτρονικών εγκλημάτων.

2.4.6 ΕΠΙΘΕΣΗ ΣΤΗ MICROSOFT

Το φθινόπωρο του 2000 έγινε ένα σοβαρό περιστατικό εισβολής σε ένα από τα πλέον γνωστά δίκτυα, αυτό της Microsoft. Χωρίς να έχουν δοθεί πολλά στην δημοσιότητα σχετικά με το τι έκαναν οι εισβολείς, το διάστημα που είχαν προσπέλαση στα συστήματα της εταιρίας (πιθανόν ποτέ δεν θα μάθουμε αν κατάφεραν να πάρουν ή να αλλάξουν τον κώδικα γνωστών προγραμμάτων), είναι σίγουρο πως η φήμη της εταιρίας δέχτηκε ένα καίριο πλήγμα.

Πέρα όμως από αυτό, ο κώδικας των προϊόντων της Microsoft είναι πολύτιμος για αρκετούς ανταγωνιστές της, που θα ήθελαν πολύ να τον έχουν στα χέρια τους. Το ζήτημα είναι πως το χτύπημα αυτό ήταν αφορμή για να χάσει η εταιρία τμήμα της πνευματικής ιδιοκτησίας της και πιθανόν της τεχνολογίας που χρησιμοποιεί. Αν πάντως οι hackers πήραν κώδικα τότε σε λίγο καιρό ή θα τον δούμε δημοσιευμένο κάπου στο διαδίκτυο ή θα πωληθεί σε όποιον δώσει τα περισσότερα.

Η επίθεση φαίνεται πως ξεκίνησε από τον υπολογιστή στο σπίτι ενός υπαλλήλου που συνδεόταν με το δίκτυο της εταιρίας. Από εκεί ένας Δούρειος Ίππος με όνομα QAZ

μεταφέρθηκε στο εσωτερικό δίκτυο της εταιρίας. Ο δούρειος αυτός ίππος μεταδίδεται μέσω ηλεκτρονικού ταχυδρομείου και αυτόματης αντιγραφής του μέσω διαμοιρασμένων φακέλων μέσα στο δίκτυο, αλλάζοντας την γνωστή εφαρμογή Notepad με τον εαυτό του.

Με την ενεργοποίηση του ο QAZ.Trojan (W32.HLLW.QAZ.A) ψάχνει για την εφαρμογή Notepad.exe και αντιγράφει τον εαυτό του στην θέση του, μετονομάζοντας το αυθεντικό σε note.exe. Κάθε φορά που κάποιος τρέχει το μεταλλαγμένο notepad.exe, εκτελείται και το note.exe, ώστε ο χρήστης να μην διαπιστώνει κάποιο πρόβλημα. Κατόπιν ψάχνει στο δίκτυο για να μολύνει και άλλα αντίγραφα του notepad.exe. Από την στιγμή που μολύνει ένα σταθμό, στέλνει με email στον hacker την IP διεύθυνση του, ενεργοποιεί το WinSock για την επικοινωνία του και περιμένει σύνδεση στο Port 7597. Απλά ο hacker ελέγχει το ηλεκτρονικό ταχυδρομείο του μέσω web, (που προφανώς έχει ανοιχτεί σε μία δωρεάν υπηρεσία με λάθος στοιχεία), και κάνει telnet από ένα άλλο κόμβο κρύβοντας με τους γνωστούς τρόπους την πραγματική του IP.

Χωρίς να έχουν δοθεί στην δημοσιότητα αρκετά στοιχεία για την δράση των εισβολέων και με αντικρουόμενες πληροφορίες για το χρονικό διάστημα που είχαν προσπέλαση στο δίκτυο (λέχθηκε για ένα μήνα ή στην καλύτερη περίπτωση για 9 μέρες), συνηθίζεται από τους hackers, τις πρώτες μέρες, να αντιγράφεται ή να αποστέλλεται με email ότι φαίνεται χρήσιμο, από τον φόβο να γίνουν αντιληπτοί (χωρίς βέβαια να μπορεί κανείς να πει πως έγινε έτσι σε αυτή την περίπτωση).

Έχει ενδιαφέρον να αναλογιστούμε πως κατάφερε ο ιός και πέρασε τα συστήματα ελέγχου της εταιρίας. Εδώ μάλλον η απάντηση βρίσκεται στον τρόπο που τα προγράμματα προστασίας ελέγχουν για ιούς. Στην πλειοψηφία τους τα προγράμματα αυτά έχουν αρχεία με τις υπογραφές των ιών που έχουν βρεθεί σε κανονική και συμπιεσμένη μορφή. Έτσι, αν για παράδειγμα συμπιεστεί ένα αρχείο που περιέχει ιό με ένα πρόγραμμα συμπίεσης, όχι ευρέως γνωστό (π.χ. NeoLite), τότε τα συστήματα προστασίας δεν το αντιλαμβάνονται αφού το αρχείο είναι εκτελέσιμο (.exe) και η υπογραφή του δεν υπάρχει μέσα σε αυτό.

Είναι λοιπόν εύκολο για οποιονδήποτε, χωρίς ιδιαίτερες γνώσεις, να συλλέξει τις πληροφορίες που χρειάζονται και να προσπαθήσει να κάνει μία επιτυχή επίθεση σε ένα ιστότοπο. Για να μπορέσει όμως να παραμείνει άγνωστη η ταυτότητα του, χρειάζεται περισσότερη εμπειρία και χρόνος.

Την επόμενη χρονιά η Microsoft ήταν πάλι στόχος των hackers. Αυτή τη φορά η επίθεση αφορούσε τα στοιχεία για το DNS της εταιρίας. Για λίγες ώρες τα στοιχεία για το DNS είχαν αλλάξει και εκατομμύρια χρήστες για δύο μέρες δεν μπορούσαν να προσπελάσουν τους web servers της.

2.4.7 ΙΩΝ ΣΥΝΕΧΕΙΑ

Στις 19 Ιουλίου 2001 το CERT/CC εκδίδει οδηγία (CA-2001-13) που αφορά το Code Red Worm. Πρόκειται για μία επίθεση Κινέζων hackers που δημιούργησε τεράστια προβλήματα τόσο σε κόμβους όσο και σε δίκτυα, δημιουργώντας μεγάλη κυκλοφορία και denial of service σε πολλά δίκτυα υπολογιστών. Ο ιός εύρισκε ένα τρωτό στον IIS 4.0 και 5.0 της Microsoft που επέτρεπε την απομακρυσμένη εκτέλεση κώδικα. Ο κώδικας αυτός μόλυνε τα συστήματα και προσπαθούσε να επεκτείνει την επίθεση και σε άλλα που βρίσκονταν κοντά τους. Σε λίγες μέρες και πριν προλάβουν να κυκλοφορήσουν οι ενημερωμένες εκδόσεις των προγραμμάτων προστασίας, τα γνωστά «αντιβιοτικά», 300,000 κόμβοι μολύνθηκαν δημιουργώντας πανικό στο διαδίκτυο. Ο ιός αυτός είχε και «μεταλλάξεις», αφού παρουσιάστηκε και σε έκδοση ΙΙ ως απάντηση από Αμερικανούς hackers, με βελτιωμένο τον

κώδικα ώστε να βρίσκει τα συστήματα που είχαν πρόβλημα και να διαδίδεται με μεγαλύτερη ταχύτητα. Ο ιός αυτός τοποθετούσε «κερκόπορτες» (backdoors) και είχε μέθοδο να εξετάζει τα συστήματα μέσα στο τοπικό δίκτυο αλλάζοντας το τελευταίο τμήμα της IP διεύθυνσης.

Ένας άλλος ιός ο W32/Sircam worm εμφανίστηκε ιδιαίτερα απειλητικός, αφού διαδιδόταν μέσω ηλεκτρονικού ταχυδρομείου με την χρήση του Outlook και μέσω διαμοιρασμένων καταλόγων (shared directories) σε συστήματα που έτρεχαν Windows. Η ευρεία διάδοσή του οφείλεται στο ότι χρησιμοποιούσε τον διευθυνσιογράφο (address book) του Outlook και έστελνε αντίγραφα σε γνωστούς με θέμα «Γεια. Πως είσαι;» και κείμενο «σου στέλνω αυτό το αρχείο και θέλω τα σχόλια σου». Ο παραλήπτης ανυποψίαστος άνοιγε το mail και το συνημμένο αρχείο με αποτέλεσμα να μολυνόταν το σύστημα του. Επίσης όταν ο κώδικας του ιού διαπίστωνε πως υπήρχε στο τοπικό δίκτυο και άλλο σύστημα με διαμοιρασμένους καταλόγους, αντέγραφε τον κώδικα του σε διάφορα σημεία του νέου συστήματος και κύρια στο βασικό αρχείο rundll32.exe και στην registry του συστήματος. Το αποτέλεσμα στα συστήματα που είχαν μολυνθεί ήταν να μην υπάρχει διασφάλιση του απορρήτου, να υπάρχει άρνηση λειτουργίας (denial of service) και απώλεια της ακεραιότητας του συστήματος. Αποτέλεσμα αυτών ήταν να αντιγραφούν παράνομα εμπιστευτικά αρχεία εταιρειών με passwords, αριθμούς πιστωτικών καρτών πελατών, σχέδια προϊόντων κ.λπ.

Μία παραλλαγή των προηγούμενων ιών ήταν το W32/Nimda@MM γνωστός απλά σαν Nimda worm. Το «σκουλήκι» αυτό χρησιμοποιούσε όλους τους τρόπους επίθεσης μέσω ταχυδρομείου, IIS web server, μόλυνση αρχείων σε file shares, ακόμα και κατεβάζοντας τον κώδικα μέσα από μολυσμένες ιστοσελίδες με απλό web-browsing. Μάλιστα, όπου εύρισκε τους προηγούμενους ιούς χρησιμοποιούσε τα τρωτά που είχαν δημιουργήσει και αφού μόλυνε τα συστήματα έκλεινε τις «τρύπες» των άλλων ιών για να μην γίνεται αντιληπτός. Ο ιός αυτός είχε σαν αποτέλεσμα την κατάρρευση πολλών δικτύων διεθνών τραπεζών.

Τέλος, το Δεκέμβριο του 2001 έκανε την εμφάνιση του ο ιός Pentagon (ή Goner) worm, γραμμένος σε Visual Basic Script (VBS), ο οποίος ήταν κάτι σαν πρόγραμμα προφύλαξης οθόνης (screen saver) που προσπαθούσε να απενεργοποιήσει τα προγράμματα προστασίας από ιούς που «έτρεχαν» στα συστήματα. Η εταιρία MessageLabs ισχυρίζεται πως σε 24 ώρες από την εμφάνιση του ιού εντόπισε 40,000 μολυσμένα συστήματα. Το αντίστοιχο για τον SirCam τον Νοέμβριο ήταν 50,000 συστήματα σε 24 ώρες.

Στον παρακάτω πίνακα (2-Α) φαίνονται οι 23 ιοί της διετίας 1999-2001 που προκάλεσαν την μεγαλύτερη κινητοποίηση ή μόλυναν τα περισσότερα συστήματα.

Όνομα ιού	Ημερομηνία ανακάλυψης	Τύπος ιού	Μέθοδος μετάδοσης	Επικινδυνότητα
W32/SirCam@MM	7/17/2001	Ιός	E-mail	Μεσαία
W32/Navidad@M	11/3/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Hybris.gen@MM	10/16/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Nimda.gen@MM	9/18/2001	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία

JS/Kak@M	10/22/1999	Ιός	VBScript Σκουλήκι	Μεσαία
VBS/VBSWG.gen@MM	2/11/2001	Ιός	VbScript	Μεσαία
W95/MTX.gen@M	8/23/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Magistr.a@MM	3/12/2001	Ιός	Σκουλήκι	Μεσαία
VBS/Loveletter@MM	5/4/2000	Ιός	VbScript	Μεσαία
W32/Naked@MM	3/6/2001	Ιός	E-mail	Μεσαία - Χαμηλή
W32/ProLin@MM	11/30/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία - Χαμηλή
W32/FunLove.4099	11/9/1999	Ιός	Win32	Μεσαία
BackDoor-G	4/15/1999	Δούρειος Ίππος	Remote Access	Μεσαία
VBS/VBSWG.Z@MM	5/16/2001	Ιός	VbScript	Μεσαία
BackDoor-Sub7	12/16/1999	Δούρειος Ίππος	Remote Access	Μεσαία
W32/CodeRed.c. Σκουλήκι	8/4/2001	Ιός	Διαδικτυακό Σκουλήκι	-
VBS/SST.gen@MM	5/9/2001	Ιός	VBScript Σκουλήκι	Μεσαία
APStrojan.qa@MM	1/18/2000	Δούρειος Ίππος	AOL Password	Μεσαία
W32/APost@MM	9/3/2001	Ιός	E-mail Σκουλήκι	Μεσαία
W32/O.A.Z.Σκουλήκι	8/7/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
IRC/Stages. Σκουλήκι	5/26/2000	Ιός	VBScript Σκουλήκι	Μεσαία
W32/Badtrans@MM	4/11/2001	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32.Pretty. Σκουλήκι .unp	2/15/2000	Δούρειος Ίππος	Σκουλήκι	Μεσαία

Πίνακας 2-Α. Λίστα με τους 23 χειρότερους ιούς

2.4.8 ΕΠΙΘΕΣΗ ΚΑΤΑ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΠΑΙΔΕΙΑΣ

Την Πέμπτη 19 Νοεμβρίου 1998, ο εξυπηρετητής του Υπουργείου Εθνικής Παιδείας και θρησκευμάτων δέχτηκε επίθεση από Έλληνες crackers, οι οποίοι και αντικατέστησαν την αρχική σελίδα με ένα κείμενο «καταγγελία». Το περιεχόμενο του web server επανήλθε στην κανονική του μορφή τις πρωινές ώρες της επόμενης μέρας.

Το κείμενο των δραστών περιείχε βολές κατά της κυβερνητικής πολιτικής στο χώρο της παιδείας, τα κόμματα της αντιπολίτευσης, τα Μέσα Μαζικής Ενημέρωσης, την Ευρωπαϊκή Ένωση, τις ειδικές δυνάμεις της αστυνομίας, τις ακροδεξιές οργανώσεις, τη Δικαιοσύνη, τον ίδιο τον Υπουργό Παιδείας και τους διάφορους «ντουντουκάδες» που κατηγορούνται ως «καπηλευτές της λαϊκής οργής».Το κείμενο συνοδευόταν από φωτογραφία συγκρούσεων μεταξύ αστυνομίας και διαδηλωτών.

Το γεγονός καλύφθηκε δημοσιογραφικά από ραδιοτηλεοπτικά μέσα ενημέρωσης. Δημοσιογραφικοί αναλυτές αναφέρουν ότι τα ορθογραφικά και συντακτικά λάθη που περιέχει το κείμενο, καταδεικνύουν το νεαρό της ηλικίας των δραστών. Η ακριβής ώρα της επίθεσης δεν είναι γνωστή, αλλά με βάση τα mails που δέχτηκε η ηλεκτρονική εφημερίδα HACK.gr, υπολογίζεται ότι η αλλαγή της σελίδας έγινε πριν από τις 11 το βράδυ της Πέμπτης.

ΕΡΟΧΗ 2021-2027

❖ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

ΚΕΦΑΛΑΙΟ 3ο

3.1 ΤΑΥΤΟΠΟΙΗΣΗ & ΠΙΣΤΟΠΟΙΗΣΗ

3.2 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

3.1 ΤΑΥΤΟΠΟΙΗΣΗ & ΠΙΣΤΟΠΟΙΗΣΗ

Για τα περισσότερα υπολογιστικά και δικτυακά συστήματα, οι διαδικασίες ταυτοποίησης και πιστοποίησης των χρηστών είναι η πρώτη γραμμή άμυνας για την ασφάλεια του συστήματος. Οι διαδικασίες ταυτοποίησης και πιστοποίησης των χρηστών έχουν σκοπό να εμποδίσουν την πρόσβαση μη εξουσιοδοτημένων χρηστών (ή διαδικασιών) στο υπολογιστικό ή δικτυακό σύστημα.

Οι διαδικασίες ταυτοποίησης και πιστοποίησης είναι ένα κρίσιμο δομικό στοιχείο της ασφάλειας ενός δικτύου δεδομένων, επειδή σε αυτές βασίζονται οι περισσότερες τεχνικές για έλεγχο πρόσβασης (access control) και σύνδεση της δραστηριότητας του συστήματος με συγκεκριμένους χρήστες που την προκάλεσαν (user accountability). Ο όρος ταυτοποίηση (identification) περιγράφει τη διαδικασία κατά την οποία ο χρήστης δηλώνει την ταυτότητα του στο σύστημα, ενώ ο όρος πιστοποίηση (authentication) περιγράφει τη διαδικασία με την οποία ο χρήστης επιβεβαιώνει τον ισχυρισμό για την ταυτότητα του.

Συνήθως η ταυτότητα ενός χρήστη δηλώνεται από έναν κωδικό ο οποίος μερικές φορές αναφέρεται και σαν όνομα εισόδου (login name) του χρήστη. Αυτή η πληροφορία μπορεί να είναι γνωστή στο διαχειριστή του συστήματος και σε όλους τους υπόλοιπους χρήστες. Π.χ. για να πιστοποιηθεί η ταυτότητα του χρήστη με όνομα εισόδου guest απαιτείται μια διαδικασία πιστοποίησης ταυτότητας (π.χ ένας κωδικός πρόσβασης - password), η οποία είναι μυστική και γνωστή μόνο στο συγκεκριμένο χρήστη. Με αυτό τον τρόπο, ο διαχειριστής συστήματος μπορεί να παρακολουθήσει τις ενέργειες του συγκεκριμένου χρήστη στο σύστημα, οι υπόλοιποι χρήστες μπορούν να ανταλλάξουν μηνύματα ηλεκτρονικού ταχυδρομείου μαζί του, κλπ., αλλά κανένας άλλος δεν μπορεί να ισχυριστεί στο σύστημα ότι είναι ο χρήστης με όνομα εισόδου guest.

Ένας μηχανισμός πιστοποίησης εξυπηρετεί στην αναγνώριση οντοτήτων με μοναδικό τρόπο και ενεργοποιείται πριν από οποιοδήποτε άλλο μηχανισμό που βασίζεται στην ταυτότητα μιας οντότητας. Επειδή η πιστοποίηση αποτελεί τη βάση για την περαιτέρω εφαρμογή άλλων μηχανισμών, απαιτείται να είναι κατά το δυνατό ασφαλέστερος και σθεναρός ο μηχανισμός που την υλοποιεί ώστε να λειτουργούν αξιόπιστα οι μηχανισμοί που βασίζονται σε αυτή.

Πριν την έναρξη της διαδικασίας πιστοποίησης, απαιτείται όλες οι οντότητες να έχουν μια μοναδική ταυτότητα. Αυτή θα πρέπει να είναι τέτοια ώστε να μην μπορεί να παραποιηθεί από άλλες οντότητες, όπως για παράδειγμα μια λέξη κλειδί που την γνωρίζει μόνο ο χρήστης, μια κάρτα (smart card) ή το δακτυλικό αποτύπωμα. Η διαχείριση των ταυτοτήτων είναι αρμοδιότητα του διαχειριστή ασφάλειας ο οποίος διατηρεί μια βάση πληροφοριών ασφάλειας η οποία είναι απαραίτητη,

Ο μηχανισμός πιστοποίησης είναι υποχρεωτικός για όλες τις οντότητες και πρέπει η ταυτότητα να αποδίδεται σε αυτές πριν την παραχώρηση των όποιων δικαιωμάτων πρόσβασης στο σύστημα. Σε πολλά συστήματα υφίστανται διαδικασίες που μεταβιβάζουν την ταυτότητα μιας οντότητας σε μια άλλη. Για παράδειγμα, όταν ένας χρήστης (οντότητα) μπει σε ένα σύστημα (login), τα δικαιώματα του κληρονομούνται σε μια ή περισσότερες διαδικασίες ή υπηρεσίες του συστήματος (άλλες οντότητες), όπως κειμενογράφους (text editors), προγράμματα αποστολής μηνυμάτων (mail programs) κλπ. Οι διαδικασίες-υπηρεσίες αυτές καλούνται κομιστές της ταυτότητας του χρήστη.

Η πιστοποίηση μπορεί να διαχωριστεί σε δύο τύπους: ***ασθενής*** και ***ισχυρή*** [NIST 800-12]:

Ασθενής ή απλή πιστοποίηση καλείται αυτή που πραγματοποιείται από απλούς μηχανισμούς που χρησιμοποιούνται από τα περισσότερα συστήματα, όπως για παράδειγμα η χρήση password όταν ένας χρήστης μπαίνει (logs in) σε ένα σύστημα.

Ισχυρή πιστοποίηση είναι αυτή που υλοποιείται μέσω μηχανισμών που δεν επιτρέπουν την αποκάλυψη του απορρήτου κατά τη διαδικασία της πιστοποίησης. Αυτό μπορεί να επιτευχθεί για παράδειγμα με τη χρήση ασύμμετρων συστημάτων κρυπτογράφησης στα οποία μόνο η οντότητα αποστολέας γνωρίζει μοναδικά πως κωδικοποιείται ένα μήνυμα αλλά όλες οι άλλες οντότητες γνωρίζουν τη διαδικασία αποκωδικοποίησης του. Στην περίπτωση αυτή καμία οντότητα δεν χρειάζεται να αποκαλύψει το κρυπτογραφικό κωδικό (κλειδί) το οποίο αποτελεί απόρρητο που δεν διαμοιράζεται σε τρίτους.

Υπάρχουν τρεις κατηγορίες συστημάτων για να πιστοποιηθεί η ταυτότητα ενός χρήστη, τα οποία μπορούν να χρησιμοποιηθούν είτε αυτόνομα είτε σε συνδυασμό:

- Συστήματα που βασίζονται σε πληροφορία / γνώση που κατέχει ο χρήστης (π.χ. κωδικός πρόσβασης, Προσωπικός Κωδικός Ταυτοποίησης (Personal Identification Number - PIN), κρυπτογραφικό κλειδί).
- Συστήματα που βασίζονται σε κάποιο αντικείμενο που κατέχει ο χρήστης (π.χ. ATM κάρτα, «έξυπνη» κάρτα - smart card).
- Συστήματα που βασίζονται σε κάποιο προσωπικό χαρακτηριστικό του χρήστη. Σε αυτή την κατηγορία ανήκουν οι μέθοδοι που βασίζονται στη βιομετρία (π.χ. έλεγχος φωνής, γραφικού χαρακτήρα, δακτυλικών αποτυπωμάτων).

Καθεμιά από τις παραπάνω μεθόδους έχει τα δικά της μειονεκτήματα, τόσο όσον αφορά την ασφάλεια, όσο και την πολυπλοκότητα χρήσης από τους εξουσιοδοτημένους χρήστες και το διαχειριστή του συστήματος. Για παράδειγμα, κάποιος θα μπορούσε να μαντέψει ή να υποκλέψει έναν κωδικό πρόσβασης, να κλέψει ή να- κατασκευάσει πλαστές ATM κάρτες, κλπ. Από την άλλη πλευρά, ένας χρήστης μπορεί να ξεχάσει τον κωδικό πρόσβασης ή να χάσει την ATM κάρτα, ενώ ο διαχειριστικός φόρτος για την παρακολούθηση των κωδικών πρόσβασης ή των καρτών μπορεί να γίνει ιδιαίτερα σημαντικός. Όσον αφορά στα συστήματα βιομετρίας, αυτά έχουν αρκετά τεχνικά προβλήματα, προβλήματα αποδοχής από την πλευρά των χρηστών, και υψηλό κόστος.

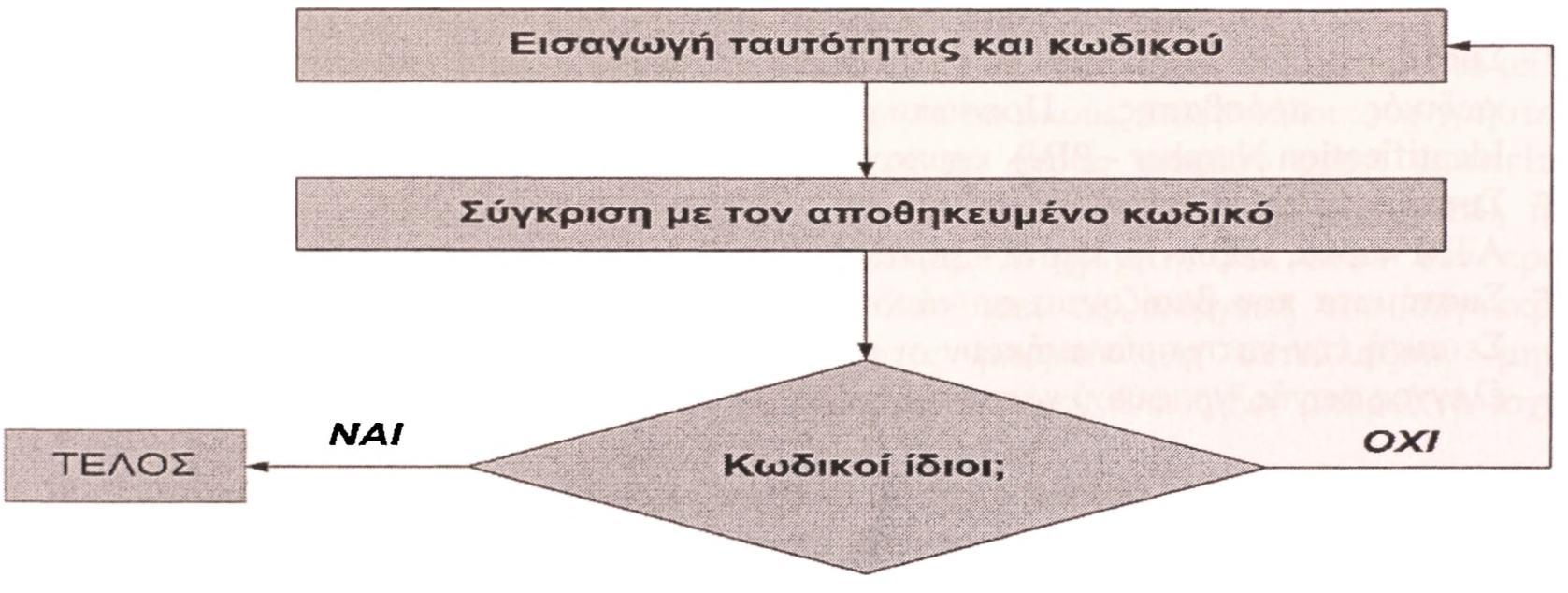
3.1.1 ΣΥΣΤΗΜΑΤΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΠΛΗΡΟΦΟΡΙΑ

Η πιο συνηθισμένη μορφή διαδικασίας ταυτοποίησης και πιστοποίησης ταυτότητας είναι ο συνδυασμός ενός ονόματος εισόδου χρήστη (login name) με μια πληροφορία που κατέχει ο χρήστης. Σε αυτή την κατεύθυνση, η σημαντικότερη κατηγορία είναι οι μηχανισμοί που βασίζονται στους συμβατικούς κωδικούς πρόσβασης (passwords).

3.1.1.1 ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ (PASSWORDS)

Τα συστήματα ταυτοποίησης και πιστοποίησης απαιτούν από το χρήστη την εισαγωγή ενός κωδικού ονόματος και ενός κωδικού πρόσβασης (ή προσωπικού κωδικού ταυτοποίησης). Το σύστημα συγκρίνει τον κωδικό πρόσβασης με έναν αποθηκευμένο κωδικό πρόσβασης που έχει συνδυαστεί με το συγκεκριμένο κωδικό όνομα. Αν οι δύο κωδικοί πρόσβασης ταυτίζονται, η ταυτότητα του χρήστη πιστοποιείται επιτυχώς, και ο χρήστης αποκτά πρόσβαση στον λογαριασμό του (Σχήμα 3-1).

Μηχανισμοί πιστοποίησης ταυτότητας βασισμένοι σε κωδικούς πρόσβασης χρησιμοποιούνται για την ασφάλεια υπολογιστικών συστημάτων εδώ και πολλά χρόνια. Τέτοιοι μηχανισμοί έχουν ενσωματωθεί σε πολλά λειτουργικά συστήματα, και τόσο οι χρήστες όσο και οι διαχειριστές συστημάτων είναι εξοικειωμένοι με αυτά. Οι μηχανισμοί που βασίζονται σε κωδικούς πρόσβασης μπορούν να παρέχουν ικανοποιητικό επίπεδο ασφάλειας, υπό την προϋπόθεση ότι διαχειρίζονται σωστά και φυλάσσονται επαρκώς.



Σχήμα 3-1: Διαδικασία ταυτοποίησης & πιστοποίησης με βάση κωδικό πρόσβασης

Η ασφάλεια ενός συστήματος που βασίζεται σε κωδικούς πρόσβασης εξαρτάται από το βαθμό που οι κωδικοί πρόσβασης παραμένουν μυστικοί. Παρόλα αυτά, υπάρχουν αρκετοί τρόποι να αποκαλυφθούν οι κωδικοί πρόσβασης:

- *Κωδικοί πρόσβασης που είναι εύκολο να μαντευθούν*. Συνήθως οι χρήστες διαλέγουν κωδικούς πρόσβασης που μπορούν να τους θυμούνται εύκολα, όπως ονόματα ατόμων, κατοικίδιων, ή αθλητικών συλλόγων. Ένας εισβολέας μπορεί εύκολα να μαντέψει έναν τέτοιου είδους κωδικό πρόσβασης. Από την άλλη πλευρά, αν οι χρήστες δυσκολεύονται να απομνημονεύσουν τους, κωδικούς πρόσβασης, τότε τους κρατούν γραμμένους σε κάποιο σημείο. Πολλά υπολογιστικά συστήματα έχουν προκαθορισμένους κωδικούς πρόσβασης για τους λογαριασμούς που χρησιμοποιούνται για τη διαχείριση του συστήματος. Επειδή αυτοί οι κωδικοί πρόσβασης είναι τυποποιημένοι, μπορούν να μαντευθούν πολύ εύκολα. Αν και αυτό το πρόβλημα έχει επισημανθεί εδώ και χρόνια, πολλοί διαχειριστές δεν έχουν αλλάξει αυτούς τους κωδικούς πρόσβασης. Ένας άλλος τρόπος για να αποκαλυφθεί ένας κωδικός πρόσβασης είναι η παρακολούθηση του χρήστη τη στιγμή που αυτός εισάγει τον κωδικό.

- *Αποκάλυψη των κωδικών πρόσβασης.* Είναι πολύ συνηθισμένο οι χρήστες να μοιράζονται τους κωδικούς πρόσβασης μεταξύ τους. Για παράδειγμα, συνάδελφοι μπορεί να γνωρίζουν ο ένας τον κωδικό πρόσβασης του άλλου, ώστε να μπορούν να μοιράζονται αρχεία και άλλους πόρους.

- *Ηλεκτρονική παρακολούθηση.* Όταν οι κωδικοί πρόσβασης μεταδίδονται στο υπολογιστικό σύστημα, μπορούν να υποκλαπούν μέσω ηλεκτρονικής παρακολούθησης του διαύλου μετάδοσης. Η παρακολούθηση μπορεί να λάβει χώρα είτε στο δικτυακό υποσύστημα που χρησιμοποιείται για τη μετάδοση, είτε στο ίδιο το υπολογιστικό σύστημα (π.χ. εγκατάσταση ενός Trojan horse). Αξίζει να σημειωθεί ότι αυτό το πρόβλημα δεν μπορεί να λυθεί με απλή κρυπτογράφηση των κωδικών πρόσβασης, γιατί κάθε φορά η κρυπτογράφηση του ίδιου κωδικού πρόσβασης δίνει το ίδιο αποτέλεσμα, οπότε ο κρυπτογραφημένος κωδικός πρόσβασης μπορεί να χρησιμοποιηθεί από κάποιον εισβολέα.

- *Πρόσβαση στο αρχείο με τους κωδικούς πρόσβασης.* Στην περίπτωση που το αρχείο με τους κωδικούς πρόσβασης των εξουσιοδοτημένων χρηστών δεν προστατεύεται επαρκώς, αυτό το αρχείο μπορεί να υποκλαπεί και να μεταφερθεί μέσω δικτύου σε άλλο, απομακρυσμένο υπολογιστικό σύστημα. Τα αρχεία με τους κωδικούς πρόσβασης σχεδόν πάντοτε προστατεύονται με τεχνικές μονόδρομης κρυπτογράφησης, ώστε οι κωδικοί πρόσβασης να μην είναι διαθέσιμοι στον διαχειριστή του συστήματος ή στους πιθανούς εισβολείς, ακόμα και αν αποκτήσουν πρόσβαση στο συγκεκριμένο αρχείο. Παρόλα αυτά, εφόσον το αρχείο με τους κωδικούς πρόσβασης μεταφερθεί σε κάποιο άλλο υπολογιστικό σύστημα, οι κρυπτογραφήσεις πολλών συμβολοσειρών μπορούν να συγκριθούν με τα περιεχόμενα του αρχείου, ώστε να ανακαλυφθούν οι κωδικοί πρόσβασης.

Με εξαίρεση την ηλεκτρονική παρακολούθηση, τα παραπάνω προβλήματα μπορούν να αντιμετωπιστούν σε σημαντικό βαθμό με σωστή πολιτική διαχείρισης των κωδικών πρόσβασης. Συνήθως επιβάλλονται κανόνες που δεν επιτρέπουν τη χρήση κωδικών που μπορούν εύκολα να μαντευθούν (π.χ. δεδομένο ελάχιστο μήκος, μίξη πεζών - κεφαλαίων και χρήση σημείων στίξης, έλεγχος με προγράμματα «σπασίματος» κωδικών πρόσβασης και συχνή αλλαγή των κωδικών). Επίσης επιβάλλονται όρια στον αριθμό των αποτυχημένων προσπαθειών για πιστοποίηση ταυτότητας, ώστε να μην διευκολύνονται οι εισβολείς στο να μαντέψουν κάποιον κωδικό πρόσβασης. Επίσης, χρησιμοποιείται μονόδρομη κρυπτογράφηση στο αρχείο των κωδικών πρόσβασης και δεν αποκλείονται οι χρήστες από κάθε πρόσβαση σε αυτό. Το πρόβλημα της ηλεκτρονικής παρακολούθησης είναι πιο σύνθετο και συνήθως λύνεται με την εφαρμογή προηγμένων μεθόδων για την πιστοποίηση ταυτότητας.

3.1.2 ΣΥΣΤΗΜΑΤΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΚΑΤΟΧΗ

Τα περισσότερα και πιο συνηθισμένα συστήματα αυτής της κατηγορίας συνδυάζουν ένα αντικείμενο που ο χρήστης έχει στην κατοχή του (π.χ. ΑΤΜ κάρτα, «έξυπνη» κάρτα) με πληροφορία που ο χρήστης γνωρίζει, ώστε να επιτύχουν μεγαλύτερη ασφάλεια από τα

συστήματα της προηγούμενης κατηγορίας. Συνήθως, το αντικείμενο που ο χρήστης έχει στην κατοχή του καλείται κουπόνι ή κάρτα (token), και τα συστήματα διακρίνονται σε αυτά που χρησιμοποιούν κάρτες μνήμης (memory tokens), και σε αυτά που χρησιμοποιούν έξυπνες κάρτες (smart tokens).

3.1.2.1 ΚΑΡΤΕΣ ΜΝΗΜΗΣ (MEMORY TOKENS)

Οι κάρτες μνήμης αποθηκεύουν, αλλά δεν επεξεργάζονται, πληροφορία. Η πιο συνηθισμένη μορφή καρτών μνήμης είναι οι μαγνητικές κάρτες (magnetic stripped cards), στις οποίες μια στενή λωρίδα μαγνητικού υλικού προσαρμόζεται στην επιφάνεια της κάρτας. Στο μαγνητικό υλικό καταγράφονται κάποιες πληροφορίες, οι οποίες αποτελούν τμήμα των δεδομένων πιστοποίησης. Η πιο συνηθισμένη χρήση αυτής της τεχνικής είναι στις Αυτόματες Ταμειακές Μηχανές (Automatic Teller Machines – ATM), στις οποίες οι μαγνητική κάρτα συνδυάζεται με τον Προσωπικό Κωδικό Ταυτοποίησης (Personal Identification Number – PIN). Σπανιότερα εφαρμόζονται διαδικασίες πιστοποίησης που βασίζονται μόνο στην κατοχή μιας κάρτας μνήμης από το χρήστη.

Είναι φανερό ότι οι διαδικασίες πιστοποίησης που βασίζονται στο συνδυασμό μιας κάρτας μνήμης με ένα PIN παρέχουν σημαντικά υψηλότερα επίπεδα ασφάλειας από τις διαδικασίες πιστοποίησης που βασίζονται μόνο σε κωδικούς πρόσβασης. Ένας εισβολέας για να προσποιηθεί ότι είναι κάποιος εξουσιοδοτημένος χρήστης πρέπει να έχει στην κατοχή του τόσο μια έγκυρη κάρτα όσο και το έγκυρο PIN για αυτή την κάρτα. Προφανώς, αυτό είναι αρκετά πιο δύσκολο από την υποκλοπή ενός κωδικού πρόσβασης, αφού τα ονόματα των χρηστών είναι διαθέσιμα σε όλους.

Παρόλα αυτά πιο σύνθετες τεχνικά επιθέσεις είναι πιθανές εναντίον ενός συστήματος που βασίζεται σε κάρτες μνήμης και PINs. Για παράδειγμα, μια ομάδα έκλεψε ένα ATM και το εγκατέστησε σε ένα εμπορικό κατάστημα. Με αυτό τον τρόπο απέκτησαν πρόσβαση σε έγκυρους αριθμούς λογαριασμών και στα αντίστοιχα PINs, κατασκεύασαν ψεύτικες κάρτες, και τις χρησιμοποίησαν για την ανάληψη χρημάτων από κανονικά ATM.

Επίσης, άλλα σημαντικά προβλήματα στη χρήση τέτοιων τεχνικών αφορούν στο κόστος, τη διαχείριση, την απώλεια των καρτών, τη δυσαρέσκεια των χρηστών, και την παραχώρηση των PINs. Συγκεκριμένα, το κόστος αυξάνεται σημαντικά από τις ειδικές συσκευές οι οποίες διαβάζουν τις μαγνητικές κάρτες, επιτρέπουν την εισαγωγή των PINs, και αποφασίζουν αν τα δεδομένα είναι έγκυρα, ώστε ο χρήστης να αποκτήσει πρόσβαση. Η απώλεια της μαγνητικής κάρτας εμποδίζει την πρόσβαση του χρήστη, μέχρι αυτή να αντικατασταθεί. Αυτό αφενός δημιουργεί επιπλέον διαχειριστικό κόστος, και αφετέρου αυξάνει τις πιθανότητες η ασφάλεια του συστήματος να παραβιαστεί από αυτόν που θα βρει το κουπόνι. Επίσης, οι χρήστες αρκετές φορές δεν καταλαβαίνουν την ανάγκη χρήσης καρτών για την πιστοποίηση ταυτότητας σε ένα υπολογιστικό σύστημα. Το φαινόμενο αυτό μπορεί να αντιμετωπιστεί με ενημέρωση των χρηστών για την αναγκαιότητα αυξημένων μέτρων για την ασφάλεια του συστήματος.

3.1.2.2 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ (SMART TOKENS)

Μια έξυπνη κάρτα επεκτείνει τη λειτουργικότητα μιας κάρτας μνήμης ενσωματώνοντας ένα ή περισσότερα ολοκληρωμένα κυκλώματα στην ίδια την κάρτα. Όταν χρησιμοποιείται

για πιστοποίηση ταυτότητας, μια έξυπνη κάρτα συνήθως συνδυάζεται με ένα PIN (ή κάποια άλλη πληροφορία). Υπάρχουν πολλοί διαφορετικοί τύποι έξυπνων καρτών, οι οποίοι διακρίνονται κυρίως με βάση τα φυσικά χαρακτηριστικά, το περιβάλλον αλληλεπίδρασης, και τα πρωτόκολλα που χρησιμοποιούνται.

Όσον αφορά στα φυσικά χαρακτηριστικά, οι έξυπνες κάρτες έχουν ενσωματωμένο ένα μικροεπεξεργαστή, ενώ τα χαρακτηριστικά μιας κατηγορίας ορίζονται σε ένα διεθνή τυποποίηση που έχει επεξεργαστεί από τον ISO.

Οι έξυπνες κάρτες έχουν είτε χειροκίνητο (manual), είτε ηλεκτρονικό περιβάλλον αλληλεπίδρασης. Στην πρώτη περίπτωση, η κάρτα έχει μικρή οθόνη ή / και πληκτρολόγιο που επιτρέπει στο χρήστη να αλληλεπιδρά με την κάρτα. Οι έξυπνες κάρτες με ηλεκτρονικό περιβάλλον αλληλεπίδρασης προσπελαύνονται (ανάγνωση / ενημέρωση / εγγραφή) μέσω ειδικών συσκευών.

Επίσης, υπάρχουν πολλοί τύποι πρωτοκόλλων που μπορούν να χρησιμοποιηθούν για πιστοποίηση με χρήση έξυπνης κάρτας. Διακρίνονται τρεις μεγάλες, γενικές κατηγορίες τέτοιων πρωτοκόλλων, τα πρωτόκολλα στατικής ανταλλαγής κωδικών πρόσβασης, τα πρωτόκολλα δυναμικής δημιουργίας κωδικών πρόσβασης, και τα πρωτόκολλα ερώτησης - απόκρισης (challenge - response).

- Οι έξυπνες κάρτες που χρησιμοποιούν στατική ανταλλαγή κωδικών πρόσβασης λειτουργούν με τρόπο παρόμοιο με αυτό των καρτών μνήμης, με μόνη διαφορά ότι πρώτα ο χρήστης πιστοποιεί την ταυτότητα του στην κάρτα, και στη συνέχεια η κάρτα αναλαμβάνει την πιστοποίηση της ταυτότητας του χρήστη στο υπολογιστικό σύστημα.
- Στην περίπτωση της δυναμικής δημιουργίας κωδικών πρόσβασης, η έξυπνη κάρτα παράγει μια συμβολοσειρά, η οποία μεταβάλλεται περιοδικά. Ανάλογα με το είδος της αλληλεπίδρασης, ο χρήστης ή η κάρτα χρησιμοποιεί αυτόν τον κωδικό για την πιστοποίηση ταυτότητας.
- Τα πρωτόκολλα ερώτησης-απόκρισης βασίζονται στην κρυπτογραφία. Το υπολογιστικό σύστημα δημιουργεί μια ερώτηση (π.χ το στιγμιότυπο ενός υπολογιστικά δύσκολου προβλήματος), και η έξυπνη κάρτα αναλαμβάνει να δώσει τη σωστή απάντηση (π.χ. τη λύση στο πρόβλημα).

Τα σημαντικότερα πλεονεκτήματα των έξυπνων καρτών είναι ότι είναι ευέλικτες και μπορούν να δώσουν λύση σε πολλά προβλήματα που σχετίζονται με την ασφάλεια των διαδικασιών πιστοποίησης. Γενικά, παρέχουν μεγαλύτερη ασφάλεια από τις μαγνητικές κάρτες, και δίνουν μια απάντηση στο πρόβλημα της ηλεκτρονικής παρακολούθησης, με τη μέθοδο των κωδικών πρόσβασης μιας χρήσης (one-time passwords). Συγκεκριμένα, οι έξυπνες κάρτες που χρησιμοποιούν πρωτόκολλα δυναμικής δημιουργίας κωδικών πρόσβασης ή ερώτησης - απόκρισης δημιουργούν κωδικούς πρόσβασης μιας χρήσης, δηλαδή κωδικούς πρόσβασης που είναι έγκυροι μόνο για τη συγκεκριμένη χρονική στιγμή. Προφανώς, η αποκάλυψη μέσω ηλεκτρονικής παρακολούθησης ενός κωδικού πρόσβασης μιας χρήσης δεν έχει νόημα, γιατί αυτός δεν μπορεί να χρησιμοποιηθεί πάλι.

Επίσης, οι έξυπνες κάρτες μειώνουν τον κίνδυνο της κατασκευής πλαστών αντιγράφων, γιατί αφενός πρόκειται για πιο σύνθετες κατασκευές, και αφετέρου η μνήμη μιας έξυπνης κάρτας δεν μπορεί να διαβαστεί, αν προηγούμενα ο χρήστης δεν πιστοποιήσει την ταυτότητα του. Ακόμη, οι έξυπνες κάρτες επιτρέπουν στους χρήστες να έχουν πρόσβαση στο σύνολο των υπολογιστικών συστημάτων ενός οργανισμού, πιστοποιώντας την ταυτότητα τους μόνο μία φορά (για το σύνολο των συστημάτων στην αρχή κάθε συνόδου. Εκτός από τις έξυπνες κάρτες, παρόμοια δυνατότητα παρέχεται από εφαρμογές που λειτουργούν σαν εξυπηρετητές

πιστοποίησης για το σύνολο των υπολογιστικών συστημάτων ενός οργανισμού, όπως το Kerberos.

Όπως και στην περίπτωση των καρτών μνήμης, τα βασικά μειονεκτήματα της χρήσης έξυπνων καρτών έχουν να κάνουν με το κόστος χρήσης και συντήρησης, και τη δυσαρέσκεια των χρηστών. Οι έξυπνες κάρτες είναι λιγότερο τρωτές στην υποκλοπή του PIN, επειδή απαιτείται από το χρήστη να πιστοποιήσει την ταυτότητα του στην ίδια την κάρτα. Από την άλλη πλευρά, οι έξυπνες κάρτες κοστίζουν περισσότερο από τις κάρτες μνήμης, και είναι πιο σύνθετες στο σχεδιασμό τους και τη λειτουργία τους.

Ένα από τα βασικά προβλήματα στη χρήση των έξυπνων καρτών είναι ότι οι αυτές που έχουν ηλεκτρονικό περιβάλλον αλληλεπίδρασης απαιτούν τη χρήση ειδικών συσκευών για ανάγνωση/εγγραφή της κάρτας, ενώ αυτές που έχουν χειροκίνητο περιβάλλον[1] αλληλεπίδρασης απαιτούν κάποιες επιπλέον ενέργειες από την πλευρά του χρήστη. Η πρώτη περίπτωση αυξάνει σημαντικά το κόστος εγκατάστασης και συντήρησης του συστήματος, ενώ η δεύτερη αυξάνει τη δυσαρέσκεια των χρηστών, που απαιτούν από τα υπολογιστικά συστήματα να είναι φιλικά προς το χρήστη. Επιπλέον, η χρήση ενός συστήματος πιστοποίησης ταυτότητας που βασίζεται σε έξυπνες κάρτες έχει σημαντικές απαιτήσεις σε διαχείριση, ενώ στην περίπτωση ταυτόχρονης χρήσης κρυπτογραφικών κλειδιών απαιτείται επιπλέον σύστημα διαχείρισης για αυτά.

3.1.3 ΣΥΣΤΗΜΑΤΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗ ΒΙΟΜΕΤΡΙΑ

Οι διαδικασίες πιστοποίησης που βασίζονται στη βιομετρία χρησιμοποιούν κάποια ατομικά χαρακτηριστικά για να πιστοποιήσουν την ταυτότητα του χρήστη. Συνήθως χρησιμοποιούνται χαρακτηριστικά όπως τα δακτυλικά αποτυπώματα, τα χαρακτηριστικά του ματιού, η χροιά της φωνής, και ο γραφικός χαρακτήρας.

Η αρχή λειτουργίας των συστημάτων βιομετρίας μπορεί να αναλυθεί σε δύο βήματα. Στη φάση αρχικοποίησης του συστήματος, δημιουργείται ένα προφίλ που περιγράφει τη μορφή του επιλεγμένου χαρακτηριστικού για κάθε χρήστη. Αυτό το προφίλ σχετίζεται με το συγκεκριμένο χρήστη και αποθηκεύεται για μελλοντική χρήση. Σε κάθε προσπάθεια πιστοποίησης, μια ειδική συσκευή ανιχνεύει τη μορφή του επιλεγμένου χαρακτηριστικού στο άτομο που προσπαθεί να αποκτήσει πρόσβαση, και εφόσον ταιριάζει με το προφίλ που έχει αποθηκευτεί, παρέχεται πρόσβαση.

Αν και τα τελευταία χρόνια τέτοιου είδους συστήματα είναι διαθέσιμα για χρήση, αυτά είναι τεχνικά πολύπλοκα και ιδιαίτερα ακριβά, ενώ σημαντικά προβλήματα μπορεί να εμφανιστούν όσον αφορά στην αποδοχή τους από τους τελικούς χρήστες. Από την άλλη πλευρά, η τεχνολογία που βασίζεται στη βιομετρία εξελίσσεται γρήγορα, και τα συστήματα γίνονται όλο και πιο αξιόπιστα, πιο φθηνά, και πιο φιλικά προς το χρήστη.

Τα συστήματα βιομετρίας μπορούν να παρέχουν πολύ υψηλό βαθμό ασφάλειας, αλλά η τεχνολογία που χρησιμοποιούν δεν είναι τόσο ώριμη όσο στην περίπτωση των καρτών μνήμης και των έξυπνων καρτών. Επιπλέον, στην περίπτωση εφαρμογής τέτοιων συστημάτων ανακύπτουν δυσκολίες που οφείλονται στο γεγονός ότι είναι δύσκολο να αποθηκευτεί για μελλοντική σύγκριση ένα ατομικό χαρακτηριστικό με ακρίβεια και λεπτομέρεια. Επίσης, κάποια ατομικά χαρακτηριστικά ενδέχεται να μεταβάλλονται σημαντικά, όπως για παράδειγμα η φωνή ενός ανθρώπου που πάσχει από κρυολόγημα ή έχει βραχνιάσει.

Εξ' αιτίας του σημαντικού κόστους και των τεχνικών δυσκολιών, αυτή τη στιγμή τα συστήματα βιομετρίας είναι κατάλληλα μόνο για περιβάλλοντα υψηλού κινδύνου, στα οποία απαιτείται πολύ υψηλός βαθμός ασφάλειας.

3.1.4 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

Η διαχείριση των δεδομένων πιστοποίησης είναι ένα από τα πιο κρίσιμα σημεία στο σχεδιασμό και τη λειτουργία ενός συστήματος πιστοποίησης. Ο φόρτος διαχείρισης σε ένα σύστημα ταυτοποίησης και πιστοποίησης ταυτότητας μπορεί να είναι ιδιαίτερα σημαντικός. Η διαχείριση συνήθως περιλαμβάνει τη δημιουργία, τη διανομή και την αποθήκευση των δεδομένων πιστοποίησης.

Για τα συστήματα που βασίζονται στους κωδικούς πρόσβασης, η διαδικασία διαχείρισης κυρίως περιλαμβάνει τον ορισμό της πολιτικής ορισμού και ανανέωσης των κωδικών πρόσβασης και τη συντήρηση του αρχείου στο οποίο αποθηκεύονται οι κωδικοί πρόσβασης. Για τα συστήματα που βασίζονται σε κουπόνια / κάρτες, η διαχείριση περιλαμβάνει τη δημιουργία και τη διανομή των καρτών και των PINs, και την εγκατάσταση και τη συντήρηση του συστήματος που θα αναγνωρίζει τα έγκυρα ζευγάρια από κάρτες και PINs. Για τα συστήματα βιομετρίας, η διαδικασία διαχείρισης κυρίως αφορά στη δημιουργία και την αποθήκευση των προφίλ των χρηστών.

Τα στοιχεία πιστοποίησης θα πρέπει να είναι μοναδικά για κάθε νόμιμο χρήστη.

Θα πρέπει απαραίτητα να ελέγχεται το μήκος των συνθηματικών που επιλέγονται από τους χρήστες. Συνθηματικά μήκους μικρότερο των έξι χαρακτήρων θα πρέπει να απαγορεύονται.

Όλοι οι χρήστες του συστήματος, εσωτερικοί ή εξωτερικοί, θα πρέπει:

- Να μην χρησιμοποιούν ως κωδικό εισόδου το login name.
- Να μην χρησιμοποιούν ως συνθηματικό το επίθετο ή το όνομα τους σε οποιαδήποτε μορφή. Επίσης δεν πρέπει να χρησιμοποιείται ως συνθηματικό το όνομα του συζύγου ή του παιδιού τους.
- Να μην χρησιμοποιούν συνθηματικά που αποτελούνται μόνο από ψηφία ή μόνο από αλφαβητικούς χαρακτήρες.
- Να μην επιλέγουν ως συνθηματικά λέξεις που περιέχονται σε λεξικό ελληνικό ή οποιασδήποτε άλλης γλώσσας.
- Να επιλέγουν συνθηματικά που είναι δύσκολο να αποκαλυφθούν.

Προκειμένου να αλλάζουν εύκολα τα συνθηματικά δεν θα πρέπει να περιλαμβάνονται στον κώδικα λογισμικού (not hard-coded). Εάν τα συνθηματικά ή οι Personal Identification Numbers δημιουργούνται μέσω του συστήματος τότε θα πρέπει να διανέμονται στους χρήστες αμέσως μετά τη δημιουργία τους και μόνο έπειτα από εντολή της διοικήσεως. Εάν τα συνθηματικά δημιουργούνται μέσω του συστήματος τότε ο αντίστοιχος αλγόριθμος δημιουργίας θα πρέπει να προστατεύεται με ύψιστα μέτρα ασφαλείας.
Άδεια χρήσης του αλγορίθμου δημιουργίας συνθηματικών θα πρέπει να έχει μόνο ο διαχειριστής του συστήματος. Επίσης επιβάλλεται κρυπτογράφηση του αλγορίθμου για την ασφαλή αποθήκευση του στα υπολογιστικά συστήματα της επιχείρησης.

Θα πρέπει να τηρείται επίσης ένα ιστορικό των συνθηματικών που έχει επιλέξει κάθε χρήστης έτσι ώστε να μην επιτρέπεται η επαναχρησιμοποίηση συνθηματικών. Το ιστορικό

θα πρέπει να περιλαμβάνει τουλάχιστον τα 5 τελευταία συνθηματικά που έχει χρησιμοποιήσει ο χρήστης. Λογαριασμοί που δεν έχουν χρησιμοποιηθεί για ένα χρονικό διάστημα μεγαλύτερο των 60 ημερών θα πρέπει να απενεργοποιούνται. Τα login names των χρηστών δεν θα πρέπει να ταυτίζονται με το πραγματικό όνομα του χρήστη αλλά θα πρέπει να ακολουθούν σειριακή αρίθμηση. Η πολιτική αυτή θα πρέπει απαραίτητα να εφαρμόζεται σε περιβάλλοντα υψηλού κινδύνου. Τα συνθηματικά δεν θα πρέπει να τυπώνονται ή να εμφανίζονται στην οθόνη σε καθαρή μορφή αλλά κωδικοποιημένα (masked). Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν κάθε τρεις μήνες, ενώ οι χρήστες των οποίων οι λογαριασμοί ανήκουν σε ομάδες με περισσότερα δικαιώματα, π.χ. διαχειριστές συστημάτων ή εφαρμογών, θα πρέπει να έχουν ξεχωριστούς κωδικούς για όλους τους υπόλοιπους λογαριασμούς τους. Οι χρήστες δεν θα πρέπει να γράφουν τους κωδικούς τους σε χαρτί και να το αφήνουν στο γραφείο τους. Ποτέ επίσης δεν θα πρέπει να αποθηκεύονται οι κωδικοί ηλεκτρονικά σε υπολογιστή ή κινητό χωρίς κρυπτογράφηση.

Ο διαχειριστής του συστήματος πρέπει να φροντίζει ώστε τα δεδομένα πιστοποίησης να είναι πάντα ενημερωμένα, προσθέτοντας, διαγράφοντας και ανανεώνοντας τα δεδομένα, ανάλογα με την κατάσταση του συστήματος. Με αυτό τον τρόπο εξασφαλίζεται ότι τα δεδομένα πιστοποίησης χρησιμοποιούνται από τους εξουσιοδοτημένους χρήστες, και όχι από άλλα άτομα τα οποία έχουν μάθει ή υποκλέψει τα δεδομένα πιστοποίησης. Επιπλέον, η διαχείριση των δεδομένων πιστοποίησης πρέπει να χειρίζεται περιπτώσεις χαμένων ή κλεμμένων κωδικών πρόσβασης ή καρτών, και περιπτώσεις κλεμμένων ή μοιραζόμενων λογαριασμών.

Μια χρήσιμη πρακτική στην κατεύθυνση της ανακάλυψης λογαριασμών που χρησιμοποιούνται από μη εξουσιοδοτημένους χρήστες είναι να πληροφορείται ο χρήστης, κατά τη διαδικασία login, πότε χρησιμοποιήθηκε ο λογαριασμός του τελευταία φορά. Στην περίπτωση που η τελευταία χρήση του λογαριασμού δεν έγινε από τον εξουσιοδοτημένο χρήστη, θα πρέπει να ενημερώνεται ο διαχειριστής του συστήματος.

Οι υπεύθυνοι ασφαλείας της εταιρίας οφείλουν σε τακτά χρονικά διαστήματα να τρέχουν προγράμματα τα οποία "σπάνε" τους κωδικούς, προκειμένου να εντοπίζουν τυχόν αδυναμίες του συστήματος και να αλλάζουν αμέσως τους κωδικούς που προσπέλασαν. Επίσης, οι χρήστες θα πρέπει να είναι ενημερωμένοι για τις δυνατότητες αυτών των προγραμμάτων, τον τρόπο λειτουργίας τους και το βαθμό επιτυχίας τους. Τέλος, κάθε σύστημα θα πρέπει να ελέγχει το περιεχόμενο του κωδικού ώστε να τον απορρίπτει εφόσον δεν πληροί τους όρους του συστήματος.

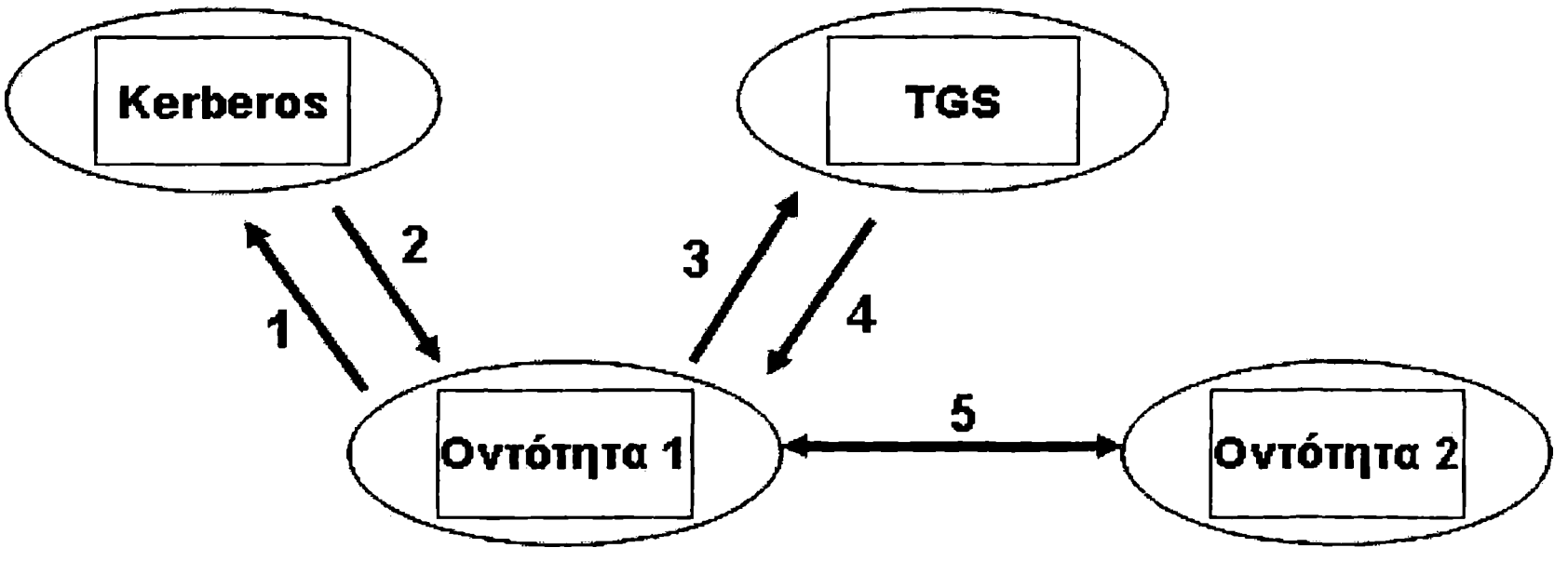
3.1.5 ΕΦΑΠΑΞ ΠΙΣΤΟΠΟΙΗΣΗ (SINGLE LOGIN)

Για λόγους αποτελεσματικότητας, είναι συχνά επιθυμητό οι χρήστες να πιστοποιούν την ταυτότητα τους εφάπαξ και στη συνέχεια να μπορούν να χρησιμοποιήσουν όλα τα υπολογιστικά συστήματα στα οποία έχουν πρόσβαση (single login), ακόμα και αν τα τελευταία απαιτούν πιστοποίηση της ταυτότητας των χρηστών. Στην περίπτωση της πρόσβασης σε διαφορετικούς πόρους του ίδιου υπολογιστικού συστήματος, ένα προηγμένο σύστημα ελέγχου πρόσβασης εύκολα μπορεί να παρέχει αυτή τη δυνατότητα. Το ίδιο δεν ισχύει στην περίπτωση ενός ετερογενούς δικτύου όπου λειτουργούν υπολογιστικά συστήματα με διαφορετικά λειτουργικά συστήματα. Διακρίνονται τρεις κατηγορίες τεχνικών για την παροχή εφάπαξ πιστοποίησης σε ετερογενή δίκτυα.

- Πιστοποίηση μεταξύ υπολογιστικών συστημάτων (host-to-host authentication): σε αυτή την κατηγορία, οι χρήστες πιστοποιούν την ταυτότητα τους εφάπαξ σε ένα κεντρικό υπολογιστικό σύστημα. Στη συνέχεια, ο κεντρικός υπολογιστής χρησιμοποιεί διάφορους μηχανισμούς (π.χ. κωδικός πρόσβασης, σύστημα ερώτησης - απόκρισης, κωδικός πρόσβασης μιας χρήσης) για να πιστοποιήσει την ταυτότητα του χρήστη στα υπόλοιπα υπολογιστικά συστήματα. Στην περίπτωση αυτή όλα τα υπολογιστικά συστήματα πρέπει να αναγνωρίζουν και να εμπιστεύονται τον κεντρικό υπολογιστή.
- Εξυπηρετητές πιστοποίησης (authentication servers): ένας εξυπηρετητής πιστοποίησης αναλαμβάνει το ρόλο του υπολογιστή στον οποίο οι χρήστες πιστοποιούν εφάπαξ την ταυτότητα τους. Προφανώς το σύνολο των υπολογιστικών συστημάτων πρέπει να εμπιστεύονται τον εξυπηρετητή πιστοποίησης, ο οποίος είναι μια εφαρμογή και δεν χρειάζεται να τρέχει σε ξεχωριστό υπολογιστή. Τυπικά παραδείγματα εξυπηρετητών πιστοποίησης είναι το Kerberos και το SPX τα οποία χρησιμοποιούν κρυπτογραφικές τεχνικές.
- Πιστοποίηση μεταξύ χρήστη και υπολογιστικού συστήματος (user-to-host authentication): σε αυτή την περίπτωση ο χρήστης πιστοποιεί την ταυτότητα του σε κάθε υπολογιστικό σύστημα ξεχωριστά. Όμως ένα κουπόνι (που μπορεί να υλοποιηθεί σαν έξυπνη κάρτα ή σαν πακέτο πληροφορίας που διακινείται στο δίκτυο) περιέχει το σύνολο των δεδομένων πιστοποίησης και διευκολύνει τη διαδικασία. Με τον τρόπο αυτό ο χρήστης έχει την εντύπωση ότι πιστοποιεί την ταυτότητα του εφάπαξ.

3.1.5.1 ΤΟ ΣΥΣΤΗΜΑ ΚΕΡΒΕΡΟΣ

Ο εξυπηρετητής τύπου *Kerberos* αρχικά υλοποιήθηκε στο MIT στα πλαίσια του project Athena. Αποτελεί ουσιαστικά ένα κεντρικό εξυπηρετητή πιστοποίησης μέσω του οποίου δημιουργούνται κλειδιά για να χρησιμοποιηθούν στη συνέχεια από διάφορες οντότητες σε επίπεδο δικτύου διασύνδεσης (network). Σε ένα τέτοιο σύστημα η ασφάλεια της διαδικασίας εξαρτάται από την ασφάλεια που παρέχει ο εξυπηρετητής και μόνο. Κάθε οντότητα έχει ένα δημόσιο κλειδί που το μοιράζεται με το σύστημα Kerberos. Αυτό το κλειδί (ή password) μεταδίδεται κατά τη διαδικασία πιστοποίησης μέσω ειδικού πρωτοκόλλου. Για να επιτευχθεί σύνδεση με άλλη οντότητα υλοποιείται η ακόλουθη διαδικασία (Σχήμα 3-2):



Σχήμα 3-2: Διαγραμματική απεικόνιση του εξυπηρετητή Kerberos

1. Η οντότητα 1 επικοινωνεί με τον Kerberos και ζητά να πιστοποιηθεί.
2. Αν ο Kerberos αποδεχθεί την οντότητα τότε της αποδίδει μια ετικέτα την οποία μπορεί να χρησιμοποιήσει για να αποδείξει την ταυτότητα της σε ένα ειδικό εξυπηρετητή, ο οποίος ονομάζεται *Ticket Granting Server* (TGS).
3. Στη συνέχεια η οντότητα 1 ζητά από τον TGS ένα κλειδί.
4. Ο TGS παραχωρεί το κλειδί για να υλοποιήσει ουσιαστικά επικοινωνία με άλλη οντότητα για παράδειγμα την οντότητα 2.
5. Το κλειδί αυτό μπορεί να χρησιμοποιηθεί ως κρυπτογραφικός κωδικός ή ως ταυτότητα κατά την επικοινωνία μεταξύ οντοτήτων.
6. Αν απαιτούνται περισσότερα κλειδιά (ταυτότητες) με σκοπό την επικοινωνία και με άλλες οντότητες, επαναλαμβάνονται μόνο τα βήματα 3 και 4.

Κατά την εκτέλεση αυτού του σεναρίου και οι δύο οντότητες γνωρίζουν ότι μόνο η αντίστοιχη τους μπορεί να επεξεργαστεί το ίδιο κλειδί (ταυτότητα). Επίσης, η οντότητα 2 μπορεί να απαγορεύσει την πρόσβαση στην οντότητα 1 διότι ο εξυπηρετητής Kerberos απλά παρέχει την υπηρεσία πιστοποίησης, δίνοντας στις οντότητες τη δυνατότητα να πιστοποιούνται μοναδικά μεταξύ τους.

Το μειονέκτημα της ανωτέρω διαδικασίας επικεντρώνεται στο ότι τα κλειδιά ταυτοποίησης αποκαλύπτονται στους τοπικούς υπολογιστές μετά τη διαδικασία πιστοποίησης και με αυτό τον τρόπο μπορούν να αποθηκευτούν και να επαναχρησιμοποιηθούν. Ένα ακόμη πρόβλημα είναι ότι ο Kerberos κατέχει όλα τα κλειδιά, για όλες τις οντότητες τα οποία πρέπει να ασφαλιστούν όσο καλύτερα γίνεται.

3.2 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

3.2.1 ΤΕΧΝΙΚΕΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Οι τεχνικές ελέγχου πρόσβασης επιτρέπουν τον έλεγχο στο είδος των υπολογιστικών πόρων ή της πληροφορίας που οι χρήστες και τα προγράμματα μπορούν να προσπελάσουν και στο είδος της προσπέλασης που μπορούν να κάνουν.

Στα πολυχρηστικά συστήματα, υπάρχουν πολλές διαφορετικές κατηγορίες υπολογιστικών πόρων και πληροφορίας αναφορικά με τα δικαιώματα προσπέλασης των χρηστών. Για παράδειγμα, υπάρχει πληροφορία που είναι προσπελάσιμη από το σύνολο των χρηστών, ευαίσθητη πληροφορία που είναι προσπελάσιμη από συγκεκριμένες ομάδες χρηστών και απόρρητη πληροφορία που είναι προσπελάσιμη μόνο από συγκεκριμένα άτομα. Επομένως, απαιτούνται διαδικασίες οι οποίες αφενός θα επιτρέπουν στους χρήστες να έχουν πρόσβαση στο σύνολο της πληροφορίας που απαιτείται για να επιτελέσουν τα καθήκοντα τους, και αφετέρου θα απαγορεύουν στους χρήστες να προσπελαύνουν οποιαδήποτε άλλη πληροφορία. Επιπλέον, είναι σημαντικό οι διαδικασίες αυτές να ελέγχουν το είδος της πρόσβασης που οι χρήστες επιτρέπεται να έχουν για κάθε είδος πληροφορία, π.χ. ανάγνωση, τροποποίηση, διαγραφή.

Ο όρος «πρόσβαση» περιγράφει τη δυνατότητα χρήσης ενός υπολογιστικού πόρου για ένα συγκεκριμένο σκοπό. «Έλεγχος πρόσβασης» είναι το σύνολο των διαδικασιών και των τεχνικών με τις οποίες η πρόσβαση παρέχεται ή απαγορεύεται. Οι διαδικασίες ελέγχου

πρόσβασης είναι τα τεχνικά μέτρα που υλοποιούν την πολιτική πρόσβασης που εφαρμόζεται για κάθε σύστημα ενός οργανισμού. Η πολιτική αυτή αποτελεί σημαντικό μέρος της πολιτικής ασφάλειας για το σύνολο του οργανισμού, και συνήθως αποφασίζεται από τους υπεύθυνους για τη λειτουργία κάθε συστήματος. Η πολιτική ελέγχου πρόσβασης πρέπει να εξισορροπεί τις συχνά αντικρουόμενες απαιτήσεις για ασφάλεια, λειτουργικότητα, και ευκολία χρήσης. Επιπλέον, η πολιτική πρέπει να εντάσσεται στο πλαίσιο ασφάλειας του οργανισμού, να είναι εφικτή τεχνικά η υλοποίηση της, και να είναι σύμφωνη με τις αποφάσεις του οργανισμού σε σχέση με τον ενδεικνυόμενο λόγο αποτελεσματικότητας/κόστους για τα μέτρα ασφάλειας που λαμβάνονται.

Οι διαδικασίες ελέγχου πρόσβασης πρέπει να καθορίζουν όχι μόνο το είδος της πρόσβασης που επιτρέπεται, αλλά και το είδος της πρόσβασης που απαγορεύεται. Οι διαδικασίες ελέγχου πρόσβασης μπορεί να υλοποιηθούν με τη βοήθεια του λειτουργικού συστήματος, λογισμικού συστήματος (π.χ. Σύστημα Διαχείρισης Βάσεων Δεδομένων, λογισμικό επικοινωνίας), προγραμμάτων εφαρμογών, ή ειδικών πακέτων για την επιβολή πολιτικής ασφάλειας, και βοηθούν σημαντικά στην προστασία:

- Του λειτουργικού συστήματος και του λογισμικού συστήματος από μη-εξουσιοδοτημένη τροποποίηση, και επομένως στη διασφάλιση της ακεραιότητας και της διαθεσιμότητας του συστήματος.
- της ακεραιότητας και της διαθεσιμότητας της πληροφορίας, περιορίζοντας τον αριθμό των χρηστών και των διαδικασιών που έχουν πρόσβαση.
- της εμπιστευτικής πληροφορίας από υποκλοπή.

Πολλές φορές οι διαδικασίες ελέγχου πρόσβασης θεωρούνται ότι αναφέρονται και εφαρμόζονται σε συστήματα αρχείων. Παρόλα αυτά οι διαδικασίες ελέγχου πρόσβασης μπορούν να χρησιμοποιηθούν για να προστατεύσουν και άλλους πόρους ενός υπολογιστικού συστήματος ή δικτύου δεδομένων, όπως για παράδειγμα τη δυνατότητα προσπέλασης σε ένα modem ή έναν εκτυπωτή. Επιπλέον, διαδικασίες ελέγχου πρόσβασης μπορούν να εφαρμοστούν σε συγκεκριμένες λειτουργίες μιας εφαρμογής ή του λειτουργικού συστήματος, και σε συγκεκριμένα πεδία μιας βάσης δεδομένων.

3.2.1.1 ΚΡΙΤΗΡΙΑ ΠΡΟΣΒΑΣΗΣ

Ένα σύστημα που υλοποιεί την πολιτική ελέγχου πρόσβασης χρειάζεται να αποφασίσει αν κάποιος χρήστης είναι εξουσιοδοτημένος να προσπελάσει χρησιμοποιήσει κάποιον υπολογιστικό πόρο. Η διαδικασία αυτή συνήθως είναι διαφορετική από τη διαδικασία ταυτοποίησης και πιστοποίησης, που αποφασίζει αν κάποιος χρήστης είναι εξουσιοδοτημένος να χρησιμοποιήσει το υπολογιστικό σύστημα για οποιαδήποτε ενέργεια.

Το σύστημα χρησιμοποιεί διάφορα κριτήρια για να αποφασίσει αν μια αίτηση για πρόσβαση θα ικανοποιηθεί ή όχι. Η πολιτική ελέγχου πρόσβασης καθορίζει το σύνολο των κριτηρίων που εξετάζονται για την πρόσβαση σε κάθε πόρο. Μερικά από τα πλέον συνηθισμένα κριτήρια πρόσβασης είναι τα ακόλουθα [NIST 800-12]:

- **Ταυτότητα:** Η πλειοψηφία των τεχνικών ελέγχου πρόσβασης βασίζεται στην ταυτότητα του χρήστη (ή της υπολογιστικής διεργασίας), η οποία εκχωρείται από το σύστημα στη φάση της ταυτοποίησης και πιστοποίησης. Πολύ συχνά οι χρήστες βάση της ταυτότητας τους, εντάσσονται σε ομάδες (groups), και η πολιτική ελέγχου

πρόσβασης καθορίζει τα δικαιώματα κάθε ομάδας (π.χ. οι χρήστες κάθε διεύθυνσης ενός οργανισμού μπορεί να έχουν πρόσβαση σε συγκεκριμένα αρχεία).

- **Αρμοδιότητα/ρόλος:** Εκτός από την ταυτότητα του χρήστη, η πρόσβαση σε υπολογιστικούς πόρους ή πληροφορία μπορεί να ελεγχθεί με βάση την αρμοδιότητα/ρόλο ενός χρήστη. Για παράδειγμα διαφορετικά δικαιώματα μπορούν να οριστούν για τους υπαλλήλους εισαγωγής στοιχείων, τους αναλυτές / προγραμματιστές, τους τμηματάρχες, και τους διευθυντές. Στην πραγματικότητα τα δικαιώματα πρόσβασης εκχωρούνται στους ρόλους (π.χ. οι αναλυτές προγραμματιστές που συντηρούν μια εφαρμογή έχουν πρόσβαση σε όλα τα αρχεία της), και το σύστημα παρέχει πρόσβαση σε όλους τους χρήστες που έχουν την αρμοδιότητα/ρόλο που απαιτείται για να προσπελαστεί κάθε συγκεκριμένος πόρος. Πρέπει να τονισθεί ότι στην περίπτωση του ελέγχου πρόσβασης με βάση τις αρμοδιότητες, η αρμοδιότητα/ρόλος κάθε χρήστη δεν αντικαθιστά την ταυτότητα του (δηλαδή δεν αρκεί κάποιος να δηλώσει στο σύστημα ότι είναι αναλυτής/προγραμματιστής), η οποία πρέπει να είναι γνωστή στο σύστημα κάθε χρονική στιγμή, ώστε να είναι εφικτή η παρακολούθηση της δραστηριότητας του συστήματος. Επίσης, σε περίπτωση σε κάποιον χρήστης έχουν ανατεθεί περισσότερες της μιας αρμοδιότητες/ρόλοι, κατά την αίτηση για πρόσβαση σε συγκεκριμένο πόρο, ο χρήστης πρέπει να δηλώνει στο σύστημα την αρμοδιότητα βάσει της οποία ζητά πρόσβαση. Για παράδειγμα, ο χρήστης που είναι επιφορτισμένος με τα καθήκοντα του διαχειριστή συστήματος πρέπει να δηλώσει αυτό στο σύστημα, ώστε να του παραχωρηθεί πρόσβαση στα αρχεία του συστήματος. Με αυτό τον τρόπο υλοποιείται η αρχή διαχωρισμού των καθηκόντων (separation of duties), σύμφωνα με την οποία κάθε χρήστης δεν επιτρέπεται να κάνει χρήση πάνω από μιας αρμοδιότητας κάθε χρονική στιγμή.
- **Τοποθεσία:** Η πρόσβαση σε συγκεκριμένους πόρους μπορεί εύκολα και αποδοτικά να ελεγχθεί με βάση τη φυσική ή λογική θέση του χρήστη που κάνει την αίτηση. Για παράδειγμα, η πρόσβαση σε συγκεκριμένους τύπους αρχείων (π.χ. αρχεία μισθοδοσίας) μπορεί να επιτρέπεται μόνο μέσω τερματικών που βρίσκονται στα κεντρικά γραφεία ενός οργανισμού, ή να απαγορεύεται σε χρήστες που έχουν συνδεθεί μέσω modem. Επίσης, η πρόσβαση σε συγκεκριμένους πόρους μέσω δικτύου μπορεί να ελέγχεται με βάση τη δικτυακή διεύθυνση του χρήστη.
- **Χρονική στιγμή:** Ο έλεγχος πρόσβασης με βάση την ώρα της ημέρας, την ημέρα της εβδομάδας, και την εβδομάδα του μήνα είναι πολύ συνηθισμένος. Για παράδειγμα, η πρόσβαση στους πόρους ενός οργανισμού μπορεί να επιτρέπεται μόνο στις εργάσιμες ώρες των εργάσιμων ημερών της εβδομάδας (π.χ. 9:00-17:00, από Δευτέρα μέχρι και Παρασκευή). Ένα άλλο παράδειγμα είναι ότι η πρόσβαση στα αρχεία μισθοδοσίας μπορεί να επιτρέπεται μόνο τις ημέρες του μήνα που παράγονται οι μισθοδοτικές καταστάσεις.
- **Περιορισμοί εξυπηρέτησης (service constraints):** Οι περιορισμοί εξυπηρέτησης αφορούν στην επιβολή κανόνων που θέτουν όρια στις υπηρεσίες που ένας πόρος μπορεί να παρέχει. Ένα τυπικό παράδειγμα περιορισμού εξυπηρέτησης είναι οι συσκευές ATM, οι οποίες δεν επιτρέπουν την ανάληψη ποσού μεγαλύτερου από κάποιο όριο. Ένα άλλο παράδειγμα είναι ο περιορισμός στον αριθμό των σελίδων που οι χρήστες μπορούν να εκτυπώσουν κάθε μήνα.
- **Τύποι πρόσβασης (access modes):** Οι τύποι πρόσβασης καθορίζουν το είδος χρήσης του υπολογιστικού πόρου ή της πληροφορίας, εφόσον η αίτηση για πρόσβαση ικανοποιηθεί. Οι πιο συνηθισμένοι τύποι πρόσβασης αφορούν την ανάγνωση, την εγγραφή, την εκτέλεση, και τη διαγραφή, και μπορούν να εφαρμοστούν τόσο σε

αρχεία του λειτουργικού συστήματος όσο και σε πληροφορία που προσπελαύνεται μέσω βάσεων δεδομένων ή εφαρμογών. Επιπλέον, σε πολλά προγράμματα εφαρμογών υπάρχει η δημιουργία νέων αντικειμένων/εγγραφών και η αναζήτηση.

3.2.1.2 ΤΕΧΝΙΚΕΣ ΥΛΟΠΟΙΗΣΗΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Υπάρχουν πολλές μέθοδοι/τεχνικές που μπορούν να χρησιμοποιηθούν για την επιβολή ελέγχου πρόσβασης σε διάφορα υπολογιστικά συστήματα ενός οργανισμού. Αυτές οι τεχνικές διαφέρουν σημαντικά μεταξύ τους όσον αφορά στο κόστος, την δυσκολία υλοποίησης και το βαθμό ασφάλειας που προσφέρουν. Επιπλέον, στις περισσότερες περιπτώσεις αυτές οι τεχνικές μπορούν να συνδυαστούν μεταξύ τους αποτελεσματικά.

Οι τεχνικές για την υλοποίηση ελέγχου πρόσβασης χωρίζονται σε δύο μεγάλες κατηγορίες: τις τεχνικές που χρησιμοποιούνται για τον έλεγχο πρόσβασης των χρηστών (ή υπολογιστικών διεργασιών) που ανήκουν στον οργανισμό (internal access controls), και τις τεχνικές που χρησιμοποιούνται για τον έλεγχο πρόσβασης των εξωτερικών χρηστών (external access controls). Στη συνέχεια δίνεται μια συνοπτική περιγραφή των πιο διαδεδομένων τεχνικών για την υλοποίηση του ελέγχου πρόσβασης [NIST 800-12]. Από αυτές οι πρώτες πέντε (κωδικοί πρόσβασης, κρυπτογράφηση, λίστες ελέγχου πρόσβασης, περιορισμένα περιβάλλοντα χρήσης, και ετικέτες ασφάλειας) αποβλέπουν κυρίως σε εσωτερικούς χρήστες, ενώ οι υπόλοιπες τρεις (συσκευές προστασίες θυρών επικοινωνίας, ασφαλείς πύλες επικοινωνίας - firewalls, και πιστοποίηση ταυτότητας βασισμένη στο υπολογιστικό σύστημα από όπου γίνεται η προσπέλαση) αποβλέπουν κυρίως σε εξωτερικούς χρήστες.

Κωδικοί Πρόσβασης (Passwords)

Η χρήση των κωδικών πρόσβασης συνήθως αφορά τις διαδικασίες ταυτοποίησης και πιστοποίησης, οι οποίες θα μπορούσαν να χαρακτηριστούν και σαν έλεγχος πρόσβασης στο ίδιο το υπολογιστικό σύστημα. Όπως σημειώθηκε στο κεφάλαιο που αναφέρεται στις διαδικασίες ταυτοποίησης και πιστοποίησης, η ευρεία χρήση κωδικών πρόσβασης για τον περαιτέρω έλεγχο πρόσβασης μπορεί να προκαλέσει σημαντική αύξηση του αριθμού των κωδικών πρόσβασης που ένας χρήστης πρέπει να γνωρίζει, ένα γεγονός που οπωσδήποτε δεν συμβάλει στη μυστικότητα των κωδικών πρόσβασης.

Παρόλα αυτά, πολλές φορές η τεχνική των κωδικών πρόσβασης χρησιμοποιείται για τον- έλεγχο πρόσβασης, ειδικά σε περιβάλλοντα δικτύων προσωπικών υπολογιστών (PCs). Η ύπαρξη κωδικού πρόσβασης στο BIOS ενός προσωπικού υπολογιστή, η χρήση κωδικού για την πρόσβαση σε διαμοιραζόμενους πόρους (shared resources) σε περιβάλλον τοπικού δικτύου, καθώς και η προστασία αρχείων με κωδικούς πρόσβασης είναι μερικά τυπικά παραδείγματα.

Η χρήση κωδικών πρόσβασης για επιβολή ελέγχου πρόσβασης είναι μια τεχνική με μικρό κόστος και εύκολη στη χρήση και τη διαχείριση, καθώς υποστηρίζεται απευθείας από το λειτουργικό σύστημα, και τόσο οι χρήστες όσο και οι διαχειριστές συστήματος είναι εξοικειωμένοι με αυτή. Από την άλλη πλευρά, εφόσον ο χρήστης έχει πρόσβαση στο λειτουργικό σύστημα είναι εύκολο να παρακάμψει τον κωδικό πρόσβασης, ενώ το πλήθος των κωδικών οδηγεί συνήθως στην καταγραφή τους από τους χρήστες.

Κρυπτογράφηση (Encryption)

Η τεχνική της κρυπτογράφησης εφαρμόζεται κυρίως σε αρχεία, και είναι ιδιαίτερα χρήσιμη για αποθήκευση πληροφορίας σε μέσα που μπορεί να χαθούν ή να κλαπούν (π.χ. δισκέτες ή φορητούς υπολογιστές). Τα κρυπτογραφημένα αρχεία μπορούν να διαβαστούν μόνο εφόσον το κλειδί για την αποκρυπτογράφηση είναι γνωστό. Η τεχνική της κρυπτογράφησης προσφέρει σημαντική ασφάλεια, και δεν είναι ιδιαίτερα ακριβή στην εφαρμογή της. Από την άλλη πλευρά, η κρυπτογράφηση των αρχείων μπορεί να επιδράσει αρνητικά στη διαθεσιμότητα, εφόσον χαθεί το κρυπτογραφικό κλειδί ή παρουσιαστεί απώλεια πληροφορίας, ενώ απαιτείται επιπλέον φόρτος για τη διαχείριση των κλειδιών. Περισσότερες λεπτομέρειες για τη χρήση κρυπτογραφικών τεχνικών παρατίθενται στο σχετικό κεφάλαιο.

Λίστες Ελέγχου Πρόσβασης (Access Control Lists – ACLs)

Μια Λίστα Ελέγχου Πρόσβασης (ΛΕΠ) είναι ένα αρχείο καταχώρησης των χρηστών (επίσης των ομάδων χρηστών, των υπολογιστών, και των υπολογιστικών διεργασιών) που έχουν πρόσβαση σε ένα συγκεκριμένο υπολογιστικό πόρο, και των τύπων της πρόσβασης που έχει κάθε χρήστης.

Οι ΛΕΠ μπορεί να ποικίλουν ως προς τις δυνατότητες και την ευελιξία τους. Μερικά είδη ΛΕΠ επιτρέπουν διαφορετικούς τύπους ελέγχου πρόσβασης /ία κάποιες συγκεκριμένες ομάδες (π.χ. κάτοχος, ομάδα κατόχου, και υπόλοιποι χρήστες), ενώ άλλα είδη ΛΕΠ επιτρέπουν περισσότερη ευελιξία, όπως ομάδες χρηστών ορισμένες από το χρήστη. Ακόμη, πιο προηγμένα είδη ΛΕΠ επιτρέπουν την άρνηση πρόσβασης σε συγκεκριμένους χρήστες ή ομάδες χρηστών.

Συγκεκριμένα, οι στοιχειώδεις ΛΕΠ (elementary access control lists) είναι συνήθως διαθέσιμες σε όλα τα πολυχρηστικά συστήματα (π.χ. UNIX). Μια στοιχειώδης ΛΕΠ είναι μια ακολουθία από δυαδικά ψηφία, η οποία ερμηνεύεται με βάση συγκεκριμένους κανόνες, και παρέχει ή όχι τη δυνατότητα πρόσβασης κάποιου χρήστη σε κάποιον υπολογιστικό πόρο.

Το πλέον τυπικό παράδειγμα στοιχειώδους ΛΕΠ, είναι οι λίστες ελέγχου πρόσβασης των αρχείων του λειτουργικού συστήματος UNIX. Για κάθε αρχείο επιβάλλονται διαφορετικοί τύποι πρόσβασης για τον κάτοχο (owner), την ομάδα χρηστών του κατόχου (group), και το σύνολο των υπόλοιπων χρηστών (world). Επίσης, για κάθε αρχείο διακρίνονται τρεις τύποι πρόσβασης: ανάγνωση, εγγραφή, και εκτέλεση. Για παράδειγμα σε ένα συγκεκριμένο αρχείο, ο κάτοχος μπορεί να έχει πλήρη δικαιώματα (ανάγνωση, εγγραφή, εκτέλεση), τα υπόλοιπα μέλη της ίδιας ομάδας χρηστών μπορεί να έχουν μόνο δικαίωμα ανάγνωσης, ενώ οι υπόλοιποι χρήστες μπορεί να μην έχουν κανένα δικαίωμα πρόσβασης.

Από την άλλη στο λειτουργικό περιβάλλον των Windows NT τα δικαιώματα διαφέρουν. Επιπλέον των τριών παραπάνω που χρησιμοποιούνται στο UNIX, υπάρχουν άλλα τρία:

- Δικαίωμα διαγραφής
- Δικαίωμα αλλαγής αδειών
- Δικαίωμα αλλαγής κατόχου

Η δυνατότητα ορισμού διαφορετικών προνομίων πρόσβασης για ομάδες χρηστών είναι ένα ιδιαίτερα χρήσιμο χαρακτηριστικό των στοιχειωδών ΛΕΠ, γιατί με αυτό τον τρόπο επιτυγχάνεται διαμοιρασμός αρχείων σε ομάδες χρηστών, χωρίς να είναι απαραίτητος ο διαμοιρασμός ενός λογαριασμού. Για παράδειγμα, με αυτό το χαρακτηριστικό, οι χρήστες που εργάζονται σε ένα συγκεκριμένο έργο μπορούν να διαμοιράσουν τα σχετικά αρχεία με

τους συναδέλφους τους, χωρίς από την άλλη πλευρά να παραχωρήσουν πρόσβαση σε αρχεία με προσωπικό περιεχόμενο, τα οποία ενδεχομένως έχουν στον λογαριασμό τους.

Οι στοιχειώδεις ΛΕΠ είναι μια απλή και ευέλικτη λύση για την υλοποίηση ελέγχου πρόσβασης. Επειδή υποστηρίζονται από όλα τα πολυχρηστικά λειτουργικά συστήματα και τα συστήματα Διαχείρισης Βάσεων Δεδομένων, το κόστος εφαρμογής και συντήρησης ενός ΛΕΠ είναι πολύ μικρό. Ένα από τα μειονεκτήματα των στοιχειωδών ΛΕΠ είναι ότι δεν επιτρέπουν το διαμοιρασμό αρχείων μεταξύ διαφορετικών ομάδων χρηστών. Επειδή κάθε χρήστης μπορεί να ανήκει σε μια μόνο ομάδα, ο μόνος τρόπος για το διαμοιρασμό αρχείων μεταξύ δυο διαφορετικών ομάδων είναι να δοθεί πρόσβαση στο σύνολο των χρηστών.

Ένα άλλο μειονέκτημα των στοιχειωδών ΛΕΠ είναι ότι δεν επιτρέπουν την άρνηση πρόσβασης σε συγκεκριμένους χρήστες. Η άρνηση πρόσβασης είναι ιδιαίτερα χρήσιμη όταν πρέπει να υλοποιηθούν εξαιρέσεις στις διαδικασίες ελέγχου πρόσβασης (π.χ. όλοι οι χρήστες της Διεύθυνσης Προσωπικού έχουν πρόσβαση στα αρχεία της Διεύθυνσης, εκτός από τη γραμματέα). Όταν δεν παρέχεται η δυνατότητα άρνησης πρόσβασης, ο μόνος τρόπος να υλοποιηθούν οι εξαιρέσεις είναι ρητώς να παραχωρηθεί πρόσβαση σε όλους του χρήστες που δικαιούνται. Αρκετές φορές αυτός ο τρόπος δεν είναι λειτουργικός, γιατί ο αριθμός των χρηστών που έχουν πρόσβαση σε σχέση με τον αριθμό των χρηστών που εξαιρούνται είναι ιδιαίτερα μεγάλος.

Τα μειονεκτήματα των στοιχειωδών ΛΕΠ καλύπτονται από τις προηγμένες ΛΕΠ (advanced access control lists), οι οποίες ακολουθούν την ίδια φιλοσοφία, αλλά επιτρέπουν λεπτομερέστερο ορισμό των ειδών πρόσβασης ανά χρήστη και ομάδες χρηστών. Στην περίπτωση των προηγμένων ΛΕΠ, υπάρχει δυνατότητα ορισμού τύπων πρόσβασης για περισσότερους του ενός μεμονωμένους χρήστες, και για περισσότερες από μία ομάδες χρηστών. Επίσης, πολλά συστήματα που υλοποιούν προηγμένες ΛΕΠ παρέχουν δυνατότητα άρνησης πρόσβασης, και υλοποίησης εξαιρέσεων. Οι προηγμένες ΛΕΠ επιτρέπουν την υλοποίηση σύνθετων πολιτικών ελέγχου πρόσβασης, αλλά η σωστή χρήση τους απαιτεί άρτια εκπαιδευμένο προσωπικό.

Περιορισμένα Περιβάλλοντα Χρήσης (Constrained User Interfaces)

Τα περιορισμένα περιβάλλοντα χρήσης χρησιμοποιούνται για να περιορίσουν την πρόσβαση των χρηστών σε συγκεκριμένη πληροφορία ή λειτουργίες αφαιρώντας από τους χρήστες τη δυνατότητα να κάνουν αίτηση για προσπέλαση αυτών των πόρων. Τρεις είναι οι βασικοί τύποι περιορισμένων περιβαλλόντων χρήσης: τα μενού (menus), οι απόψεις βάσεων δεδομένων (database views), και τα φυσικά περιορισμένα περιβάλλοντα (physically constrained user interfaces).

Τα μενού είναι πολύ συνηθισμένοι τύποι περιορισμένων περιβαλλόντων χρήσης, όπου διαφορετικοί χρήστες προσπελαύνουν το ίδιο σύστημα μέσα από διαφορετικά μενού, και επομένως μπορούν να εκτελέσουν διαφορετικά σύνολα ενεργειών ή εντολών ή να προσπελάσουν διαφορετική πληροφορία. Τα μενού προσομοιώνουν σε σημαντικό βαθμό το μοντέλο με το οποίο λειτουργεί ένα υπολογιστικό σύστημα. Στα περισσότερα υπολογιστικά συστήματα, οι διαχειριστές μπορούν να περιορίσουν την πρόσβαση των χρηστών στο λειτουργικό σύστημα ή σε συγκεκριμένες εντολές. Οι χρήστες μπορούν να εκτελέσουν μόνο τις εντολές που έχει επιτρέψει ο διαχειριστής. Ένας άλλος τρόπος περιορισμού των εντολών που οι χρήστες μπορούν να εκτελέσουν είναι η χρήση περιορισμένων shells. Η χρήση των μενού και των περιορισμένων shells συχνά διευκολύνει τη χρήση του συστήματος, και μειώνει την πιθανότητα και τις συνέπειες των λαθών από την πλευρά των χρηστών.

Οι απόψεις βάσεων δεδομένων είναι ένας μηχανισμός που περιορίζει την πρόσβαση των χρηστών στα δεδομένα μιας βάσης. Ο μηχανισμός των διαφορετικών απόψεων ανά χρήστη ή ομάδα χρηστών χρησιμοποιείται στην περίπτωση που κάποιος χρήστης χρειάζεται να έχει πρόσβαση σε μια βάση δεδομένων, αλλά δεν απαιτείται να έχει πρόσβαση στο σύνολο της. Ο μηχανισμός των απόψεων μπορεί να υλοποιήσει πολύπλοκα σενάρια ελέγχου πρόσβασης, τα οποία συχνά ανακύπτουν σε περιβάλλοντα μεγάλων βάσεων δεδομένων. Για παράδειγμα, αν κάποιος υπάλληλος ασχολείται με τη μισθοδοσία του προσωπικού κάποιων συγκεκριμένων διευθύνσεων, αυτός χρειάζεται να έχει πρόσβαση μόνο στις αντίστοιχες εγγραφές, και όχι στο σύνολο της βάσης δεδομένων του προσωπικού.

Τέλος, τα φυσικά περιορισμένα περιβάλλοντα επίσης περιορίζουν τις λειτουργίες που μπορούν να εκτελέσουν οι χρήστες. Τυπικό παράδειγμα είναι οι συσκευές ATM, οι οποίες επιτρέπουν στους χρήστες την εισαγωγή μόνο αριθμητικών χαρακτήρων, έχοντας μόνο αριθμητικό πληκτρολόγιο.

Ετικέτες Ασφάλειας (Security Labels)

Μια ετικέτα ασφάλειας είναι ένας χαρακτηρισμός που έχει αποδοθεί σε ένα υπολογιστικό πόρο, όπως για παράδειγμα ένα αρχείο. Οι ετικέτες μπορούν να χρησιμοποιηθούν για ποικίλους σκοπούς, όπως έλεγχο πρόσβασης, καθορισμό προστατευτικών μέτρων, ή παροχή οδηγιών χρήσης. Στις περισσότερες εφαρμογές/υλοποιήσεις, οι ετικέτες που χρησιμοποιούνται δεν μπορούν να μεταβληθούν, παρά μόνο κάτω από ελεγχόμενες συνθήκες ή ύστερα από διαδικασία αξιολόγησης και αναθεώρησης των μέτρων ασφάλειας.

Στην περίπτωση του ελέγχου πρόσβασης, ετικέτες μπορούν να ανατεθούν σε συνόδους χρηστών (user sessions). Κάθε χρήστης μπορεί να αρχικοποιήσει συνόδους με συγκεκριμένες ετικέτες. Επιπλέον, για κάθε ετικέτα υπάρχει ένα συγκεκριμένο σύνολο από χρήστες που μπορεί να αρχικοποιήσει αντίστοιχες συνόδους. Οι ετικέτες της συνόδου και των αρχείων που προσπελάστηκαν χρησιμοποιούνται επίσης για να καθορίσουν τις ετικέτες των πιθανών αποτελεσμάτων της συνόδου (π.χ νέα αρχεία που προήλθαν από την επεξεργασία άλλων κατά τη διάρκεια της συνόδου). Με αυτό το τρόπο εξασφαλίζεται ότι η πληροφορία προστατεύεται με ομοιόμορφο τρόπο σε όλο τον κύκλο ζωής του συστήματος.

Ο μηχανισμός των ετικετών αποτελεί μια πολύ ισχυρή τεχνική ελέγχου πρόσβασης. Από την άλλη πλευρά, ο μηχανισμός των ετικετών έχει συνήθως υψηλό κόστος, και απαιτεί σημαντικό διαχειριστικό φόρτο, επομένως είναι κατάλληλος για συστήματα με υψηλές απαιτήσεις από πλευράς ασφάλειας. Το σημαντικότερο πλεονέκτημα του μηχανισμού των ετικετών είναι ότι έχουν μόνιμη σύνδεση με την πληροφορία ή τους υπολογιστικούς πόρους. Επιπλέον, η σύνδεση διατηρείται κατά την αντιγραφή της πληροφορίας, και κληρονομείται κατά την επεξεργασία της. Επομένως, ακόμα και αν ένας εξουσιοδοτημένος χρήστης αντιγράψει στο λογαριασμό του ένα αρχείο με ετικέτα υψηλού βαθμού ασφάλειας, δεν μπορεί να μεταβάλει την ετικέτα αυτού του αρχείου (όπως θα μπορούσε στην περίπτωση των ΛΕΠ), ώστε να παρέχει πρόσβαση μέσω του λογαριασμού του και σε άλλες ομάδες χρηστών.

Συσκευές Προστασίας Θυρών Επικοινωνίας (Port Protection Devices – PPDs)

Αυτές οι συσκευές προστασίας εφαρμόζονται σε θύρες επικοινωνίας και αναλαμβάνουν τον έλεγχο πρόσβασης των χρηστών σε αυτές. Μια τέτοια συσκευή προστασίας μπορεί να είναι ξεχωριστή ή ενσωματωμένη στην θύρα επικοινωνίας, και συνήθως απαιτεί από τους

χρήστες να πιστοποιήσουν την ταυτότητα τους με κάποιο μηχανισμό (π.χ. κωδικούς πρόσβασης) για να αποκτήσουν πρόσβαση στη θύρα επικοινωνίας.

Ένα τυπικό παράδειγμα μηχανισμού προστασίας θυρών επικοινωνίας είναι το dial-back modem. Στην περίπτωση του dial-back modem, ο χρήστης καλεί τη συσκευή και πιστοποιεί την ταυτότητα του με έναν κωδικό πρόσβασης. Στη συνέχεια, το modem κλείνει τη σύνδεση, και εφόσον ο χρήστης είναι εξουσιοδοτημένος, το modem αναλαμβάνει να καλέσει τον αριθμό τηλεφώνου που αντιστοιχεί στο συγκεκριμένο χρήστη. Αυτή η πολιτική προστατεύει από μη εξουσιοδοτημένη πρόσβαση, ακόμη και στην περίπτωση υποκλοπής του κωδικού πρόσβασης. Οι επίδοξοι εισβολείς θα πρέπει να χρησιμοποιήσουν τεχνικές όπως μεταγωγή ή εκτροπή κλήσεων, για να αποκτήσουν πρόσβαση στο modem.

Ασφαλείς Πύλες (Secure Gateways) – Πυρότοιχοι (Firewalls)

Οι ασφαλείς πύλες επικοινωνίας (secure gateways), οι οποίες συχνά ονομάζονται απλώς πυρότοιχοι (firewalls), παρεμβάλλονται μεταξύ ενός ιδιωτικού δικτύου δεδομένων και ενός μεγαλύτερου, συνήθως δημοσίου δικτύου, και έχουν σαν στόχο την προστασία του ιδιωτικού δικτύου από εισβολείς (hackers). Τα συστήματα πυρότοιχων επιτρέπουν στους χρήστες του εσωτερικού δικτύου να συνδεθούν στο εξωτερικό δίκτυο, και ταυτόχρονα ελέγχουν την πρόσβαση των εξωτερικών χρηστών στο εσωτερικό δίκτυο.

Τα firewalls διαμορφώνονται ώστε να φιλτράρουν την κυκλοφορία που σχετίζεται με ενδεχόμενα τρωτά σημεία του συστήματος, ή είναι ύποπτη για ενδεχόμενη εισβολή στο σύστημα. Για παράδειγμα, ένας πυρότοιχος μπορεί να φιλτράρει την κυκλοφορία που σχετίζεται με απομακρυσμένη πρόσβαση ή εκτέλεση εντολών σε κάποιο υπολογιστικό σύστημα του εσωτερικού δικτύου. Άλλοι πυρότοιχοι απαγορεύουν κάθε είδος κυκλοφορίας, εκτός από συγκεκριμένα είδη (π.χ. ηλεκτρονικό ταχυδρομείο, WWW), ενώ άλλα εφαρμόζουν έλεγχο πρόσβασης με βάση τη διεύθυνση του κόμβου από όπου γίνεται η πρόσβαση.

Επειδή οι πυρότοιχοι ουσιαστικά παρέχουν έλεγχο πρόσβασης περιορίζοντας την κυκλοφορία ή τις υπηρεσίες που παρέχονται, μπορεί να επηρεάσουν σημαντικά τη διαθεσιμότητα και τη χρήση του συστήματος. Επομένως για την εγκατάσταση και τη λειτουργία ενός πυρότοιχου χρειάζεται να ληφθούν αποφάσεις σε επίπεδο πολιτικής ασφάλειας, οι οποίες αφορούν την εξισορρόπηση των παρεχόμενων υπηρεσιών, του κόστους του συστήματος ασφάλειας και του βαθμού ασφάλειας του συστήματος. Οι αποφάσεις σε επίπεδο πολιτικής καθορίζουν τις υπηρεσίες που θα παρέχονται στους χρήστες του εξωτερικού δικτύου, το συνολικό κόστος του πυρότοιχου, και την εργασία που θα διατίθεται για τη διαχείριση ενός τέτοιου συστήματος. Αφού παρθούν οι αποφάσεις σε επίπεδο πολιτικής, οι τεχνικές αποφάσεις συνίστανται στην επιλογή της αρχιτεκτονικής και των προϊόντων που υλοποιούν με βέλτιστο τρόπο τη δεδομένη πολιτική.

Η υλοποίηση ενός πυρότοιχου έχει σημαντικά πλεονεκτήματα για έναν οργανισμό. Συγκεκριμένα, η σωστή εγκατάσταση, και η προσεκτική συντήρηση ενός πυρότοιχου μειώνει σημαντικά τους κινδύνους εξωτερικής εισβολής και επιτρέπει την επικέντρωση της προσπάθειας για αναβάθμιση του επιπέδου ασφάλειας στα υπολογιστικά συστήματα που αποτελούν τον πυρότοιχο. Με αυτό τον τρόπο ο πυρότοιχος αποτελεί ένα κομβικό σημείο για την παροχή και διαχείριση διαφόρων υπηρεσιών, και την ενίσχυση της ασφάλειας του συστήματος. Για παράδειγμα, οι WWW, FTP και SMTP εξυπηρετητές συνήθως λειτουργούν σε υπολογιστικά συστήματα που εντάσσονται στην αρχιτεκτονική του πυρότοιχου, ενώ μέτρα που εφαρμόζονται για να αναβαθμίσουν την ασφάλεια του συστήματος (π.χ. προηγμένες τεχνικές πιστοποίησης ταυτότητας) μπορούν να εφαρμοστούν μόνο σε αυτό το σημείο.

Πιστοποίηση Ταυτότητας Βασισμένη στο Υπολογιστικό Σύστημα (Host – Based Authentication)

Σε αυτή την τεχνική, η πιστοποίηση της ταυτότητας και η παροχή πρόσβασης βασίζεται στην ταυτότητα (π.χ. δικτυακή διεύθυνση) του υπολογιστικού συστήματος από το οποίο προέρχεται η αίτηση για πρόσβαση. Πολλές δικτυακές εφαρμογές χρησιμοποιούν τη δικτυακή διεύθυνση του συστήματος από το οποίο γίνεται η αίτηση για να αποφασίσουν αν θα ικανοποιήσουν την αίτηση για πρόσβαση. Για παράδειγμα, οι εξυπηρετητές Δικτυακού Συστήματος Αρχείων (Network File System) επιτρέπουν σε υπολογιστές με συγκεκριμένες δικτυακές διευθύνσεις να προσπελάσουν συγκεκριμένους λογικούς δίσκους και καταλόγους.

Το βασικό μειονέκτημα αυτής της τεχνικής είναι εύκολα κάποιος υπολογιστής μπορεί να διαμορφωθεί σαν να διαθέτει μια από τις διευθύνσεις που επιτρέπουν την πρόσβαση. Βέβαια υπάρχουν μηχανισμοί (π.χ. Secure Remote Procedure Call που χρησιμοποιεί τον κρυπτογραφικό αλγόριθμο DES) που παρέχουν ασφαλή αναγνώριση της ταυτότητας του απομακρυσμένου κόμβου.

ΚΕΦΑΛΑΙΟ 4

4.1 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

4.2 ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

4.3 ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ (AUDITING)

4.4 ΕΝΗΜΕΡΩΣΗ ΤΩΝ ΧΡΗΣΤΩΝ

4.5 ΧΕΙΡΙΣΜΟΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

4.6 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ

4.7 ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΚΑΤΑΣΤΡΟΦΗΣ

4.1 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

4.1.1 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Για να είναι επιτυχής η πολιτική ασφάλειας θα πρέπει να γίνει αξιολόγηση και κατηγοριοποίηση της ευαισθησίας των δεδομένων και των διαθέσιμων εφαρμογών. Προφανώς θα πρέπει να κοινοποιηθεί σε όλους τους υπαλλήλους το επίπεδο ασφάλειας που απαιτείται ανά κατηγορία δεδομένων και ανά εφαρμογή.

Η επιχείρηση θα πρέπει να αξιολογήσει κάθε πληροφορία που έχει στη διάθεση της ανάλογα με την ευαισθησία που τη διακρίνει ως εμπιστευτική, ευαίσθητη, δημόσια, ή ιδιωτική. Συγκεκριμένα:

Εμπιστευτική: Είναι πληροφορία *πολύ ευαίσθητη* για την επιχείρηση και ορίζεται αυστηρά μόνο για εσωτερική χρήση. Οποιαδήποτε αποκάλυψή της θα αποβεί εξαιρετικά επιζήμια για την επιχείρηση.

Ευαίσθητη: Απαιτείται έλεγχος της ακεραιότητας προκειμένου να προστατευτεί η πληροφορία αυτή από τροποποίηση ή διαγραφή. Απαιτείται επισταμένη προσοχή για την ακρίβεια και την πληρότητα της πληροφορίας αυτής.

Προσωπική: Πρόκειται για προσωπικές πληροφορίες που η αποκάλυψή τους θα επηρεάσει αρνητικά την επιχείρηση και τους εργαζόμενους.

Δημόσια: Είναι οι πληροφορίες που δεν εντάσσονται στις άλλες κατηγορίες και η αποκάλυψή τους δεν αναμένεται να επηρεάσει την επιχείρηση ή τους εργαζομένους της.

4.1.2 ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Όλες οι πληροφορίες που έχουν αποθηκευτεί στο δίκτυο της επιχείρησης αποτελούν περιουσιακό στοιχείο της επιχείρησης. Οι πληροφορίες και το λογισμικό της επιχείρησης δεν θα πρέπει να πωλούνται η να διατίθονται σε τρίτους εκτός εάν έχει δοθεί σχετική άδεια από τη διοίκηση. Όλα τα μηνύματα που μεταφέρονται μέσω του δικτύου της επιχείρησης αποτελούν περιουσιακό στοιχείο της επιχείρησης. Η διοίκηση έχει το δικαίωμα να εξετάζει τα δεδομένα που αποθηκεύονται ή μεταφέρονται μέσω του δικτύου. Τα προσωπικά στοιχεία των εργαζομένων, των συνεργατών ή των συμβούλων της επιχείρησης δεν θα πρέπει να αποθηκεύονται στο δίκτυο εκτός εάν σχετίζονται άμεσα με την εργασία που επιτελείται στα πλαίσια της επιχείρησης. Οι πληροφορίες που συλλέγονται για τους πελάτες, τους υποψήφιους πελάτες ή τους προμηθευτές (π.χ. διεύθυνση, τηλέφωνο κλπ.) θα πρέπει να χρησιμοποιούνται μόνο στα πλαίσια της επιχείρησης. Τα μηνύματα που μεταφέρονται στο εσωτερικό της επιχείρησης αλλά και μεταξύ επιχείρησης και πελάτη ή προμηθευτή θα πρέπει να προσπελάζονται μόνο από τον αποστολέα και τον παραλήπτη του μηνύματος ενώ επιτρέπεται αποκάλυψη του μηνύματος μόνο όταν συντρέχουν λόγοι ασφάλειας.

4.1.3 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Όλες οι πληροφορίες της επιχείρησης θα πρέπει να προστατεύονται προκειμένου να μην αποκαλυφθούν σε τρίτες οντότητες. Η αποκάλυψη κάποιας πληροφορίας της επιχείρησης σε τρίτη οντότητα θα πρέπει να γίνεται μόνο έπειτα από έγκριση της διοίκησης. Εάν υπάρχει υποψία αποκάλυψης ευαίσθητων ή εμπιστευτικών πληροφοριών της επιχείρησης τότε θα πρέπει να ενημερώνονται άμεσα οι διαχειριστές του συστήματος και οι υπεύθυνοι ασφαλείας. Οι εργαζόμενοι δεν θα πρέπει να αποκαλύπτουν σε τρίτους τις λεπτομέρειες υλοποίησης του συστήματος ασφαλείας εκτός εάν τους έχει δοθεί σχετική άδεια. Οι πληροφορίες για την άδεια πρόσβασης στα υπολογιστικά και επικοινωνιακά συστήματα της επιχείρησης, όπως τα user-ids και οι dial-up αριθμοί τηλεφώνου δεν θα πρέπει να είναι προσβάσιμα από μη εξουσιοδοτημένες οντότητες. Πληροφορίες σχετικά με ευπάθειες η αδυναμίες του συστήματος θα πρέπει να γνωστοποιούνται *μόνο* στους διαχειριστές του συστήματος και στους υπεύθυνους ασφαλείας. Οι εργαζόμενοι της επιχείρησης δεν θα πρέπει να αποκαλύπτουν σε τρίτους τις ευπάθειες του συστήματος διότι εκθέτουν όλη την επιχείρηση σε κίνδυνο. Αντίθετα η επιχείρηση θα πρέπει να παρουσιάζει μία εικόνα προς τα έξω που εμπνέει ασφάλεια και όχι ανησυχίες. Η εκτύπωση ευαίσθητης και εμπιστευτικής πληροφορίας θα πρέπει να γίνεται σε εκτυπωτή ο οποίος δεν είναι συνδεδεμένος στο δίκτυο της επιχείρησης. Όταν εκτυπώνεται εμπιστευτική ή ευαίσθητη πληροφορία τότε ο εκτυπωτής θα πρέπει να είναι υπό επιτήρηση έως ότου περατωθεί η εκτύπωση. Εάν κατά την εκτύπωση της ευαίσθητης πληροφορίας παρατηρηθεί δυσλειτουργία στον εκτυπωτή τότε απαιτείται να διαγραφεί η εκτύπωση και να καταστραφούν οι άχρηστες σελίδες.

4.1.4 ΑΚΕΡΑΙΟΤΗΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η διοίκηση θα πρέπει να πιστοποιεί την ακεραιότητα, ακρίβεια και εγκυρότητα των πληροφοριών που λαμβάνονται υπόψη στη λήψη αποφάσεων. Σε περίπτωση που υπάρχει ακόμα και υποψία αποτυχίας του ελέγχου ακεραιότητας των πληροφοριών αυτών θα πρέπει άμεσα να ενημερώνεται η διοίκηση. Προτού μεταδοθεί μία πληροφορία μέσω του δικτύου θα πρέπει να έχει προηγούμενα πιστοποιηθεί η ακρίβεια και η εγκυρότητά της. Η επιχείρηση θα πρέπει να χρησιμοποιεί μηχανισμούς μέσω των οποίων πιστοποιείται η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους μέσω του δικτύου. Προτού εισαχθεί μία πληροφορία σε ένα σύστημα πολλαπλών χρηστών θα πρέπει να υφίσταται έλεγχο εγκυρότητας και ακρίβειας.

4.2 ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

Προκειμένου να προστατευτεί το λογισμικό που χρησιμοποιεί η επιχείρηση θα πρέπει να ελέγχεται η πρόσβαση των χρηστών στα υπολογιστικά συστήματα της επιχείρησης. Για την ασφάλεια του λογισμικού και των δεδομένων θα πρέπει να δοθούν οδηγίες για τον καθορισμό των δικαιωμάτων πρόσβασης. Επίσης θα πρέπει να οριστεί και η πολιτική εισαγωγής λογισμικού στο δίκτυο της επιχείρησης καθώς και η πολιτική πρόληψης, ανίχνευσης και διαγραφής ιομορφών.

4.2.1 ΚΑΘΟΡΙΣΜΟΣ ΔΙΚΑΙΩΜΑΤΩΝ ΠΡΟΣΒΑΣΗΣ

Οι χρήστες που έχουν τη δυνατότητα να προσπελάσουν πληροφορίες συγκεκριμένου επιπέδου ευαισθησίας θα πρέπει να επιτρέπεται να έχουν πρόσβαση μέσω του δικτύου και σε πληροφορίες που έχουν αξιολογηθεί ως λιγότερο ευαίσθητες [Wood91]. Σε όλους τους χρήστες θα πρέπει να δίδονται μόνο τα δικαιώματα πρόσβασης που είναι απαραίτητα για τη διεκπεραίωση της εργασίας τους (need to know). Η διοίκηση της επιχείρησης θα πρέπει να ορίσει ποια άτομα έχουν πρόσβαση σε ποιες πληροφορίες καθώς και τους περιορισμούς χρήσης των πληροφοριών της επιχείρησης. Η πρόσβαση των χρηστών στις πληροφορίες για τις οποίες έχουν εξουσιοδοτηθεί θα πρέπει να περιορίζεται σε συγκεκριμένες ώρες της ημέρας, συγκεκριμένες ημέρες της εβδομάδας και από συγκεκριμένους σταθμούς εργασίας. Η διοίκηση της επιχείρησης θα πρέπει να ορίσει τα άτομα εκείνα που έχουν το δικαίωμα να τροποποιήσουν ή να διαγράψουν συγκεκριμένους τύπους πληροφοριών. Όταν οι απλοί χρήστες δεν έχουν σχετική εξουσιοδότηση δεν θα πρέπει να προσπελάζουν πληροφορίες ιδιοκτησίας άλλων χρηστών. Μόνο οι διαχειριστές του συστήματος και οι υπεύθυνοι ασφαλείας επιτρέπεται να προσπελάζουν τα αρχεία των χρηστών. Τα δικαιώματα πρόσβασης των χρηστών θα πρέπει να αναθεωρούνται από τη διοίκηση τουλάχιστον ανά εξάμηνο. Η διοίκηση θα πρέπει να ενημερώνει τους διαχειριστές του συστήματος με όλες τις σημαντικές αλλαγές στα καθήκοντα των εργαζομένων διότι ενδέχεται να απαιτείται και τροποποίηση των δικαιωμάτων πρόσβασης. Οι εξωτερικοί χρήστες εξουσιοδοτούνται να αποκτήσουν πρόσβαση στα συστήματα της επιχείρησης μόνο έπειτα από έγγραφη έγκριση της διοίκησης.

4.2.2 ΕΛΕΓΧΟΣ ΕΙΣΑΓΩΓΗΣ ΛΟΓΙΣΜΙΚΟΥ

Οι δοκιμαστικές εκδόσεις λογισμικού θα πρέπει να διαγράφονται από το σύστημα όταν εκπνεύσει η περίοδος δοκιμής ή θα πρέπει να ακολουθηθεί η σχετική διαδικασία προκειμένου η επιχείρηση να γίνει νόμιμος κάτοχος του προϊόντος. Ο διαχειριστής του συστήματος θα πρέπει κάθε εξάμηνο να διανέμει στους χρήστες μία λίστα με τα προγράμματα που έχουν αναπτυχθεί in-house και δίνουν ανταγωνιστικό πλεονέκτημα στην επιχείρηση. Το λογισμικό που χρησιμοποιεί η επιχείρηση θα πρέπει να εγκαθίσταται μόνο από το διαχειριστή του συστήματος και από εξουσιοδοτημένους υπαλλήλους. Ο διαχειριστής του συστήματος θα πρέπει να ελέγχει περιοδικά εάν η επιχείρηση είναι νόμιμος κάτοχος του λογισμικού που χρησιμοποιεί. Σε περίπτωση που κάποιος υπάλληλος παραβιάσει την πολιτική αυτή θα πρέπει να υφίσταται τις σχετικές συνέπειες. Όλα τα προγράμματα αλλά και η τεκμηρίωση των προγραμμάτων αποτελούν περιουσιακό στοιχείο της επιχείρησης. Η διοίκηση θα πρέπει να διαθέτει στοιχεία βάσει των οποίων πιστοποιείται ότι η επιχείρηση είναι νόμιμος κάτοχος των προγραμμάτων και των εφαρμογών που χρησιμοποιεί. Θα πρέπει να ελέγχεται περιοδικά από το διαχειριστή του συστήματος ή τους υπεύθυνους ασφαλείας η συμμόρφωση με τους όρους των συμφωνιών που έχουν υπογραφεί με τους προμηθευτές του λογισμικού. Οι διαχειριστές του συστήματος θα πρέπει να ελέγχουν περιοδικά του σκληρούς δίσκους των μικροϋπολογιστών και των σταθμών εργασίας των χρηστών προκειμένου να ελεγχθεί εάν έχει εγκατασταθεί λογισμικό για το οποίο η επιχείρηση δεν είναι νόμιμος κάτοχος. Η αντιγραφή του λογισμικού θα πρέπει να πραγματοποιείται μόνο εάν επιτρέπεται από τον προμηθευτή του λογισμικού.

Οι εργαζόμενοι στα πλαίσια της επιχείρησης δεν θα πρέπει να κατέχουν λογισμικό το οποίο αποκαλύπτει συνθηματικά ή βοηθά στην κρυπτανάλυση των κρυπτογραφημένων δεδομένων. Τέτοια εργαλεία θα πρέπει να χρησιμοποιούνται μόνο από τους διαχειριστές του συστήματος. Οι χρήστες θα πρέπει να εκπαιδευτούν στη χρήση εργαλείων ανίχνευσης ιών. Το λογισμικό ανίχνευσης ιών θα πρέπει να εγκατασταθεί στους εξυπηρετητές αρχείων (file servers) προκειμένου να περιοριστεί η μετάδοση του ιού στο δίκτυο. Οι εργαζόμενοι θα πρέπει να ενημερώνουν τον διαχειριστή του συστήματος για τυχόν μη αναμενόμενη συμπεριφορά του συστήματος ή κάποιας εφαρμογής που χρησιμοποιούν. Όταν ενημερωθεί ο διαχειριστής του συστήματος για την εισβολή κάποιου ιού θα πρέπει να ενημερώνει όλους τους χρήστες που έχουν πρόσβαση στο «μολυσμένο σύστημα» ότι υπάρχει πιθανότητα μετάδοσης του ιού. Οποιοσδήποτε υπολογιστής είναι μολυσμένος θα πρέπει άμεσα να αποσυνδέεται από το δίκτυο. Ο υπολογιστής δεν θα πρέπει να επανασυνδέεται στο δίκτυο έως ότου ο διαχειριστής του συστήματος πιστοποιήσει ότι η διαγραφή του ιού έχει ολοκληρωθεί με επιτυχία.

4.3 ΚΑΤΑΓΡΑΦΗ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ (AUDITING)

Η ενίσχυση της ασφάλειας σε ένα δικτυακό τόπο επιβάλει τον ορισμό των διαδικασιών συλλογής δεδομένων που παράγονται από τη δικτυακή δραστηριότητα σε ένα ιστότοπο. Η ανάλυση των δεδομένων αυτών μπορεί να αποβεί χρήσιμη στην αντιμετώπιση προβλημάτων που μπορεί να προκύψουν από την παραβίαση της ασφάλειας του.

4.3.1 ΤΙ ΣΥΛΛΕΓΕΤΑΙ

Τα δεδομένα που συλλέγονται πρέπει να περιλαμβάνουν κάθε προσπάθεια παραβίασης των επιπέδων ασφάλειας από ένα άτομο, διεργασία ή άλλη οντότητα του δικτύου [RFC 2196]. Αυτό περιλαμβάνει είσοδο στο σύστημα (login), έξοδο από το σύστημα (logout), πρόσβαση με δικαιώματα «super user», δημιουργία εισιτηρίων (π.χ για το Kerberos) και κάθε άλλη δραστηριότητα κατά τη διαδικασία πρόσβασης ή αλλαγή της κατάστασης. Είναι ιδιαίτερα σημαντικό να καταγράφεται πότε γίνεται «anonymous» ή «guest» πρόσβαση σε δημόσιους εξυπηρετητές.

Τα στοιχεία που πρέπει να συγκεντρωθούν δεν είναι απαραίτητα τα ίδια για όλους τους ιστότοπους και για διαφορετικούς τύπους προσβάσεων μέσα στον ίδιο ιστότοπο. Γενικότερα, η πληροφορία που πρέπει να συλλεχθεί περιλαμβάνει: όνομα χρήστη (username) και όνομα υπολογιστή (hostname) για είσοδο (login) και έξοδο (logout), δικαιώματα προηγούμενης και νέας πρόσβασης για αλλαγή των δικαιωμάτων πρόσβασης, και χρονοσφραγίδα (timestamp). Φυσικά, υπάρχει πολύ περισσότερη πληροφορία που μπορεί να συγκεντρωθεί, και η οποία εξαρτάται από το τι κάνει το σύστημα και πόσος είναι ο προσφερόμενος χώρος για την αποθήκευση της συλλεγόμενης πληροφορία. Είναι πολύ σημαντικό να μη συγκεντρώνονται πληροφορίες για τους κωδικούς πρόσβασης. Αυτό δημιουργεί ενδεχόμενη καταπάτηση της ασφάλειας αν οι συλλεγόμενες εγγραφές προσπελαύνονται από μη εξουσιοδοτημένους χρήστες.

4.3.2 ΔΙΑΔΙΚΑΣΙΑ ΛΗΨΗΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (Backups)

Μια κλασική διαδικασία που εφαρμόζεται σε υπολογιστικά συστήματα είναι αυτή της λήψης αντιγράφων ασφαλείας. Για να είναι σωστός ο σχεδιασμός που γίνεται για την ασφάλεια ενός δικτυακού τόπου, η διαδικασία λήψης αντιγράφων θα πρέπει να αποτελεί αναπόσπαστο κομμάτι του. Κατά την δημιουργία αντιγράφων ασφαλείας θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα [RFC 2196]:

- Να είναι δυνατή η δημιουργία αντιγράφων ασφαλείας.
- Τα αντίγραφα θα πρέπει να αποθηκεύονται έξω από το δικτυακό τόπο (off-site). Ο αποθηκευτικός χώρος θα πρέπει να επιλέγεται προσεκτικά σύμφωνα με τα ακόλουθα κριτήρια: την ασφάλεια και τη διαθεσιμότητα του.
- Προκειμένου να έχουμε επιπρόσθετη ασφάλεια τα αντίγραφα θα πρέπει να κρυπτογραφούνται. Η ανάκτηση της πληροφορίας θα πρέπει να είναι δυνατή από οποιαδήποτε σημείο οποιαδήποτε στιγμή. Επίσης άμεσα διαθέσιμα θα πρέπει να είναι και τα προγράμματα αποκρυπτογράφησης.
- Τα αντίγραφα ασφαλείας ενδεχομένως να μην περιέχουν τη σωστή πληροφορία. Πολλές φόρες μπορεί να γίνεται η λήψη ενός αντιγράφου ενώ η πληροφορία έχει υποστεί αλλοίωση.
- Τα αντίγραφα θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα τόσο για την ορθότητα όσο και για την πληρότητα τους.

4.4 ΕΝΗΜΕΡΩΣΗ ΤΩΝ ΧΡΗΣΤΩΝ

Όλοι οι εργαζόμενοι, οι εξωτερικοί χρήστες, οι σύμβουλοι και οι συνεργάτες της επιχείρησης θα πρέπει να ενημερωθούν για την πολιτική ασφαλείας που ακολουθείται. Ο υπεύθυνος για την ανάπτυξη της πολιτικής ασφαλείας θα πρέπει να βεβαιωθεί ότι αντίγραφο της πολιτικής ασφάλειας δικτύου είναι διαθέσιμο σε όλους τους χρήστες. Το έγγραφο που θα διανεμηθεί θα πρέπει να φέρει την υπογραφή της διοικήσεως. Μετά την πάροδο ενός μήνα, θα πρέπει να συγκεντρωθούν οι απορίες των χρηστών προκειμένου να διευκρινισθούν τυχόν ασάφειες στην πολιτική ασφαλείας. Θα πρέπει να οργανωθούν σεμιναριακά προγράμματα παρουσίασης των θεμάτων που καλύπτονται στην πολιτική ασφαλείας. Βασικός στόχος των προγραμμάτων εκπαίδευσης είναι να αντιληφθούν οι χρήστες με ποιο τρόπο η πολιτική ασφαλείας προστατεύει τα περιουσιακά στοιχεία της επιχείρησης. Βασικά θέματα που πρέπει να καλυφθούν είναι :

- Ασφάλεια των Δεδομένων.
- Ασφάλεια του λογισμικού.
- Ευθύνες και Υποχρεώσεις.
- Πολιτική ασφάλειας διαδικτύου.
- Χειρισμός των ατυχημάτων ασφαλείας κ.λ.π.

Μετά την ολοκλήρωση των σεμιναρίων οι υπεύθυνοι ασφαλείας θα πρέπει να εξετάσουν εάν οι χρήστες έχουν επαρκώς κατανοήσει την πολιτική ασφαλείας. Στη συνέχεια θα πρέπει να δοθεί ένα χρονικό διάστημα προσαρμογής, όχι περισσότερο από δύο μήνες και έπειτα θα

πρέπει να ζητηθεί από τους χρήστες να υπογράψουν σχετικό έγγραφο στο οποίο θα αναφέρεται ότι μελέτησαν την πολιτική ασφάλειας δικτύου και ότι αποδέχονται ανεπιφύλακτα την τήρηση της. Μετά από κάθε αναθεώρηση της πολιτικής ασφαλείας θα πρέπει να ακολουθείται η διαδικασία εκπαίδευσης των χρηστών που αναφέρθηκε. Ανεξάρτητα από το εάν έχει γίνει ή όχι αναθεώρηση της πολιτικής ασφαλείας θα πρέπει ετησίως να οργανώνονται σεμινάρια με θέμα την ανάγκη τήρησης της πολιτικής ασφαλείας της επιχείρησης. Ο υπεύθυνος ασφαλείας θα πρέπει να διανείμει αντίγραφο της πολιτικής ασφάλειας δικτύου σε κάθε νέο υπάλληλο της επιχείρησης. Στα πλαίσια εκπαίδευσης του νέου υπαλλήλου θα πρέπει να ενταχθεί και το θέμα της ασφάλειας. Επιβάλλεται οι εξωτερικοί χρήστες να λάβουν γνώση για την πολιτική ασφαλείας που ακολουθείται από την επιχείρηση. Επίσης, πριν δοθεί άδεια πρόσβασης στο δίκτυο της επιχείρησης θα πρέπει ο εξωτερικός χρήστης να δεσμευτεί ότι θα ακολουθεί την πολιτική ασφαλείας. Ο εξωτερικός χρήστης θα πρέπει να πειστεί ότι για το χρονικό διάστημα που έχει πρόσβαση στο δίκτυο της επιχείρησης θα αντιμετωπίζεται όπως κάθε άλλος χρήστης της επιχείρησης και επιβάλλεται να σέβεται την πολιτική ασφαλείας διαφορετικά θα επιβληθούν οι κυρώσεις που προβλέπονται από τους νόμους (π.χ. νόμο περί πνευματικής ιδιοκτησίας).

Ειδικά για τους εξωτερικούς χρήστες της επιχείρησης στο πρόγραμμα εκπαίδευσης θα πρέπει να δοθεί βαρύτητα στα εξής θέματα:

- Πολιτική ασφάλειας διαδικτύου.
- Ασφάλεια δεδομένων.
- Πολιτική ελέγχου πρόσβασης.

4.5 ΧΕΙΡΙΣΜΟΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (INCIDENT HANDLING)

4.5.1 ΑΝΤΑΠΟΚΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η ανταπόκριση της ασφάλειας υπολογιστών στις απειλές έχει γίνει ένα σημαντικό συστατικό των προγραμμάτων πληροφορικής [NIST 800-61]. Οι σχετικές με την ασφάλεια απειλές έχουν γίνει όχι μόνο πιο πολυάριθμες και διαφορετικές αλλά και πιο καταστρεπτικές και αποδιοργανωτικές. Νέοι τύποι περιστατικών σχετικά με την ασφάλεια προκύπτουν συχνά. Οι προληπτικές δραστηριότητες βασισμένες στα αποτελέσματα των αξιολογήσεων του κινδύνου μπορούν να μειώσουν τον αριθμό των περιστατικών, αλλά δεν μπορούν να αποτρέψουν όλα τα περιστατικά. Μια ικανότητα ανταπόκρισης είναι επομένως απαραίτητη για να ανιχνεύσει γρήγορα τα περιστατικά, ελαχιστοποιώντας τις απώλειες και καταστροφές, μετριάζοντας τις αδυναμίες που εκμεταλλεύτηκαν και αποκαθιστώντας τις υπολογιστικές υπηρεσίες. Με αυτό το στόχο, η δημοσίευση παρέχει τις οδηγίες για το χειρισμό περιστατικών, ιδιαίτερα για την ανάλυση των σχετικών στοιχείων του περιστατικού και τον καθορισμό της κατάλληλης ανταπόκρισης σε κάθε περιστατικό. Οι οδηγίες μπορούν να ακολουθηθούν ανεξάρτητα από συγκεκριμένες πλατφόρμες υλικού, λειτουργικά συστήματα, πρωτόκολλα, ή αιτήσεις.

Επειδή η αποτελεσματική εκτέλεση της ανταπόκρισης σε ένα περιστατικό είναι σύνθετη διαδικασία, η καθιέρωση μιας επιτυχούς ικανότητας ανταπόκρισης απαιτεί ουσιαστικό

προγραμματισμό και πόρους. Ο συνεχής έλεγχος των απειλών μέσω των Συστημάτων Ανίχνευσης Εισβολών (Intrusion Detection Systems – IDSs) και άλλων μηχανισμών είναι απαραίτητος. Η καθιέρωση των σαφών διαδικασιών για τον τρέχοντα και πιθανό επιχειρησιακό αντίκτυπο των περιστατικών είναι κρίσιμη, όπως και το να εφαρμόζονται αποτελεσματικοί μέθοδοι συλλογής, ανάλυσης και αναφοράς δεδομένων. Η δημιουργία σχέσεων και η καθιέρωση των κατάλληλων τρόπων επικοινωνίας με άλλες εσωτερικές ομάδες (π.χ., ανθρώπινο δυναμικό, νομικό) και με τις εξωτερικές ομάδες (π.χ., άλλες συναφείς ομάδες ανταπόκρισης, επιβολή νόμου) είναι επίσης ζωτικής σημασίας.

Η οργάνωση μιας αποτελεσματικής ικανότητας ανταπόκρισης περιστατικού για την ασφάλεια υπολογιστών (CSIRC – Computer Security Incident Response Capability) περιλαμβάνει διάφορες σημαντικές αποφάσεις και ενέργειες. Μια από τις πρώτες εκτιμήσεις είναι να δημιουργηθεί ένας ειδικός οργανισμός για τον συγκεκριμένο καθορισμό του όρου "περιστατικό" έτσι ώστε το πεδίο του όρου να είναι σαφές. Η οργανισμός πρέπει να αποφασίσει ποιες υπηρεσίες η ομάδα ανταπόκρισης πρέπει να παρέχει, να εξετάσει ποιες δομές ομάδων και ποια πρότυπα μπορούν να παρέχουν αυτές τις υπηρεσίες και να επιλέξει και να εφαρμόσει μια ή περισσότερες ομάδες ανταπόκρισης. Η πολιτική ανταπόκρισης και η δημιουργία διαδικασίας είναι ένα σημαντικό μέρος της καθιέρωσης μιας ομάδας, έτσι ώστε η ανταπόκριση να εκτελείται αποτελεσματικά, αποδοτικά και με συνέπεια. Οι πολιτικές και οι διαδικασίες πρέπει να απεικονίζουν τις αλληλεπιδράσεις της ομάδας με άλλες ομάδες μέσα στην οργανισμό καθώς επίσης και με τις εξωτερικά συμβαλλόμενες ομάδες, όπως η επιβολή νόμου, τα μέσα μαζικής ενημέρωσης, και άλλες οργανισμούς ανταπόκρισης.

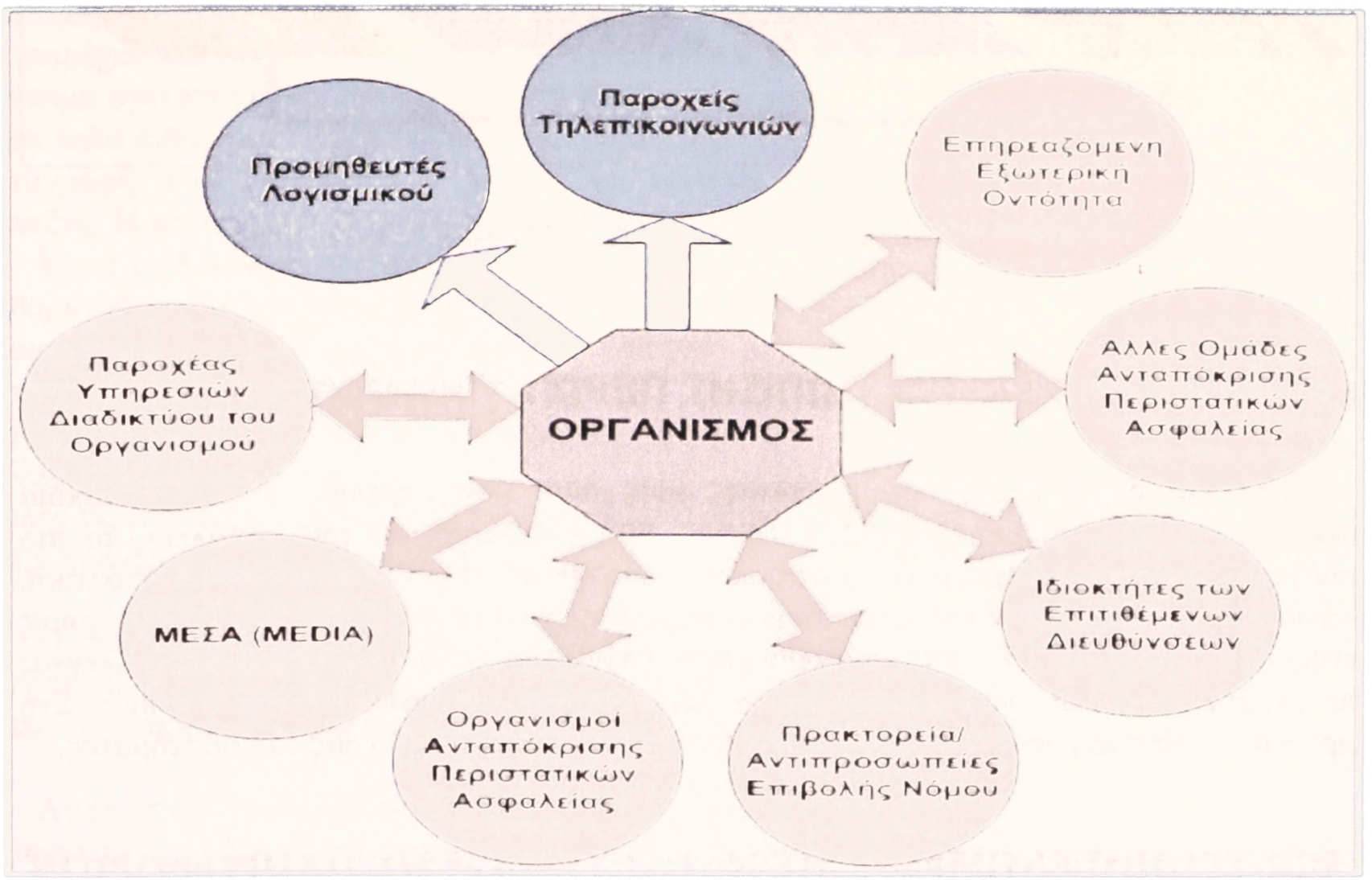
4.5.1.1 «ΚΥΚΛΟΣ ΖΩΗΣ» ΚΑΙ ΣΥΜΒΑΛΛΟΜΕΝΕΣ ΟΜΑΔΕΣ

Ο οργανισμός μπορεί να πρέπει να επικοινωνήσει με τα εξωτερικά συμβαλλόμενα μέρη σχετικά με ένα περιστατικό ασφάλειας. Αυτό περιλαμβάνει υποβολή εκθέσεων των γεγονότων στις οργανώσεις όπως το Ομοσπονδιακό Κέντρο Ανταπόκρισης Προβλημάτων Υπολογιστών (FedCIRC) και το Κέντρο Συντονισμού CERT ® (CERT ® / CC), που έρχεται σε επαφή με την επιβολή νόμου και που τοποθετεί τις έρευνες από τα μέσα (media). Αυτοί που χειρίζονται προβλήματα ασφάλειας μπορεί επίσης να πρέπει να συζητήσουν το γεγονός με άλλα συμβαλλόμενα μέρη όπως π.χ ο Φορέας Παροχής Υπηρεσιών Διαδικτύου του οργανισμού (Internet Service Provider – ISP), τον φορέα παροχής υπηρεσιών που ο επιτιθέμενος χρησιμοποιεί, τον προμηθευτή ενός τρωτού λογισμικού ή άλλες ομάδες ανταπόκρισης περιστατικών ασφαλείας οι οποίες μπορεί να είναι εξοικειωμένες με την ασυνήθιστη δραστηριότητα που ο χειριστής ενός προβλήματος προσπαθεί να κατανοήσει.

Ένας οργανισμός μπορεί να θελήσει -ή απαιτείται- να επικοινωνήσει με έναν εξωτερικό οργανισμό σχετικά με τις λεπτομέρειες ενός περιστατικού ασφαλείας για πολλούς λόγους. Η ομάδα ανταπόκρισης περιστατικών ασφαλείας πρέπει να συζητήσει αυτό επί μακρόν με το γραφείο δημοσίων υποθέσεων της οργάνωσης, το νομικό τμήμα, και τη διαχείριση πριν εμφανιστεί ένα περιστατικό ασφάλειας, για να καθιερώσει τις πολιτικές και τις διαδικασίες σχετικά με τη διανομή πληροφοριών. Διαφορετικά, ευαίσθητες πληροφορίες σχετικές με τα περιστατικά ασφάλειας μπορεί να παρασχεθούν σε αναρμόδια μέρη, κάτι που θα οδηγούσε σε μεγαλύτερη διάσπαση και οικονομικές απώλειες από ότι το ίδιο το περιστατικό ασφάλειας. Η ομάδα ανταπόκρισης θα πρέπει να τεκμηριώσει όλες τις επαφές και τις επικοινωνίες με τα εξωτερικά συμβαλλόμενα μέρη για λόγους ευθύνης και απόδειξης.

Στο παρακάτω σχήμα (σχήμα 4-1) φαίνεται η επικοινωνία ενός οργανισμού με εξωτερικά συμβαλλόμενα μέρη όπως οι προμηθευτές λογισμικού (software vendors), ο

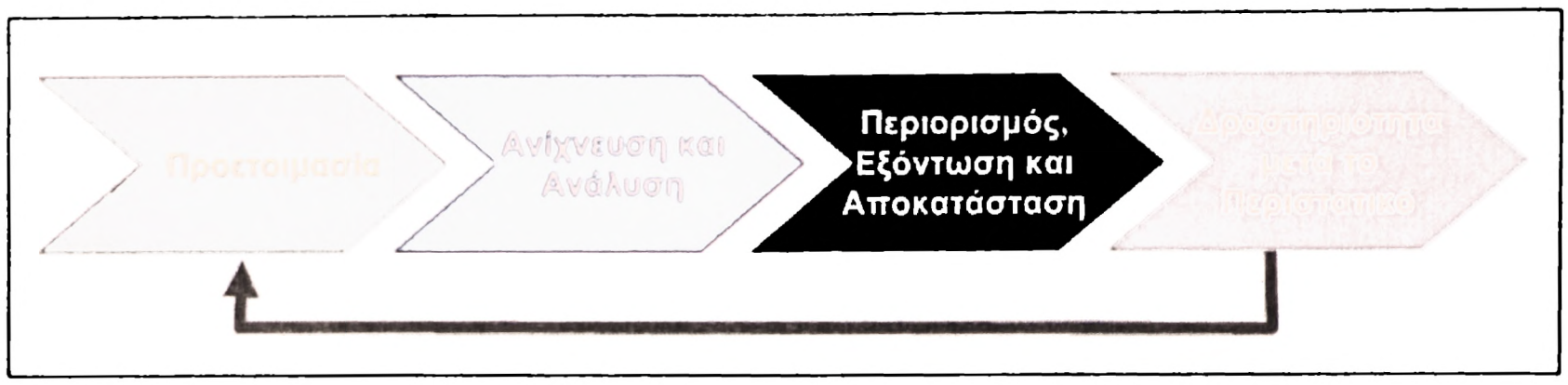
παροχέας τηλεπικοινωνιών (telecommunication provider), ο παροχέας υπηρεσιών διαδικτύου (internet service provider-ISP), τα «μέσα» (media), άλλες ομάδες ανταπόκρισης περιστατικών ασφαλείας, επηρεαζόμενα εξωτερικά μέρη κλπ.



Σχήμα 4-1: Εξωτερικά συμβαλλόμενες ομάδες

Η διαδικασία ανταπόκρισης περιστατικού έχει διάφορες φάσεις, από την αρχική προετοιμασία μέχρι την μετά-περιστατικού ανάλυση [NIST 800-61].

Η αρχική φάση περιλαμβάνει την καθιέρωση και την κατάρτιση μιας ομάδας ανταπόκρισης περιστατικού, και την απόκτηση των απαραίτητων εργαλείων και πόρων. Κατά τη διάρκεια της προετοιμασίας, η οργάνωση προσπαθεί επίσης να περιορίσει τον αριθμό περιστατικών που θα εμφανιστούν με την επιλογή και την εφαρμογή ενός συνόλου ελέγχων βασισμένων στα αποτελέσματα των αξιολογήσεων του κινδύνου. Η ανίχνευση των παραβιάσεων ασφάλειας είναι απαραίτητη για να προειδοποιήσει τον οργανισμό όποτε τα γεγονότα εμφανίζονται. Ανάλογα με τη σοβαρότητα του περιστατικού , ο οργανισμός μπορεί να ενεργήσει για να μετριάσει τον αντίκτυπο του περιστατικού με τον περιορισμό του και με την τελική ανάκτηση από αυτό. Αφότου αντιμετωπιστεί επαρκώς το περιστατικό, ο οργανισμός εκθέτει μια αναφορά που απαριθμεί την αιτία και το κόστος του περιστατικού και των βημάτων που οι οργανισμοί πρέπει να ακολουθήσουν για να αποτρέψουν τα μελλοντικά περιστατικά. Οι σημαντικότερες φάσεις της διαδικασίας ανταπόκρισης ενός περιστατικού είναι: **προετοιμασία** (preparation), **ανίχνευση και ανάλυση** (detection and analysis), **περιορισμός/εξόντωση/αποκατάσταση** (containment/eradication/recovery), **δραστηριότητα μετά το περιστατικό** (post-incident activity). Οι φάσεις αυτές φαίνονται στο παρακάτω σχήμα (σχήμα 4-2).



Σχήμα 4-2: Ο «κύκλος ζωής» ενός περιστατικού ασφάλειας

4.5.2 ΠΟΛΙΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Κατά τη διάρκεια της αντιμετώπισης μίας παραβίασης πρέπει να γίνουν κάποια συγκεκριμένα βήματα. Σε όλες τις ενέργειες που σχετίζονται με την ασφάλεια, το πιο σημαντικό πράγμα που πρέπει γίνει, είναι όλοι οι δικτυακοί τόποι να έχουν από μία πολιτική. Χωρίς καθορισμένες πολιτικές και στόχους, οποιεσδήποτε ενέργειες θα παραμείνουν χωρίς αντίκρισμα. Ένας από τους πιο καθοριστικούς στόχους είναι να αποκατασταθεί ο έλεγχος των προσβεβλημένων συστημάτων και να περιοριστούν οι συνέπειες και η ζημιά. Στη χειρότερη περίπτωση, ίσως να επιβάλλεται και η διακοπή της λειτουργίας του συστήματος.

4.5.2.1 ΤΡΟΠΟΙ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΑΝΤΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Όταν επιβεβαιωθεί μία παραβίαση, πρέπει να ειδοποιηθεί το κατάλληλο προσωπικό. Η διαδικασία με την οποία επιτυγχάνεται αυτή η ενημέρωση είναι πολύ σημαντική για τη διατήρηση της κατάστασης υπό έλεγχο, τόσο από τεχνικής όσο και από συναισθηματικής άποψης. Οι περιστάσεις πρέπει να περιγραφούν όσο το δυνατόν πιο λεπτομερειακά, με σκοπό την άμεση αναγνώριση και κατανόηση του προβλήματος. Πρέπει να δοθεί ιδιαίτερη προσοχή στον καθορισμό των ομάδων που δίνονται οι λεπτομερείς τεχνικές πληροφορίες κατά τη διάρκεια της ειδοποίησης (π.χ. είναι πολύ σημαντικό να δίνονται τέτοιου είδους πληροφορίες σε ομάδα αντιμετώπισης παραβιάσεων παρά να διατεθεί σε newsgroups ή mailing lists).

Καταρχήν, κάθε ειδοποίηση σε προσωπικό εντός ή εκτός του δικτυακού τόπου πρέπει να είναι σαφής. Αυτό απαιτεί κάθε ανακοίνωση (είτε είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου, είτε ένα τηλεφώνημα κ.λ.π.) που παρέχει πληροφορία για την παραβίαση να είναι καθαρή, σύντομη και σαφής. Μία άλλη σημαντική θεώρηση όταν επικοινωνούμε για μία παραβίαση είναι η απόδοση της πραγματικότητας. Το να γίνονται προσπάθειες απόκρυψης στοιχείων της παραβίασης με το να παρέχονται λάθος ή ελλιπείς πληροφορίες μπορεί όχι μόνο να εμποδίσει μία επιτυχή ανάλυση της παραβίασης, αλλά μπορεί και να χειροτερέψει την κατάσταση. Η επιλογή της γλώσσας που χρησιμοποιείται κατά την ενημέρωση για την παραβίαση μπορεί να έχει μία δυσκολονόητη επίδραση στον τρόπο που δίνεται η πληροφορία. Όταν χρησιμοποιούνται συναισθηματισμοί ή εμπρηστικοί όροι, αυξάνεται η πιθανότητα ζημιάς και αρνητικής έκβασης της υπόθεσης. Είναι πολύ σημαντική η διατήρηση της ψυχραιμίας τόσο στις γραπτές όσο και στις προφορικές επικοινωνίες.

4.5.2.2 ΠΡΟΦΥΛΑΞΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ/ΑΡΧΕΙΩΝ ΤΗΣ ΕΠΙΘΕΣΗΣ

Όταν αντιμετωπιστεί αποτελεσματικά μία παραβίαση, θα πρέπει να τηρείται ένα λεπτομερές αρχείο με οποιαδήποτε πληροφορία σχετίζεται με την παραβίαση. Αυτό μπορεί να παρέχει μια πολύ σημαντική βοήθεια ώστε να διαλευκανθεί μια σειρά γεγονότων σε σύντομο σχετικά χρόνο. Αν για παράδειγμα δεν γίνει καταγραφή όλων των τηλεφωνημάτων, είναι πολύ πιθανόν να παραβλεφθεί ένα σημαντικό κομμάτι πληροφορίας. Την ίδια στιγμή, η καταγραφή των παραβιάσεων μπορεί να παρέχει τεκμήρια σε περίπτωση δικαστικής διένεξης. Η καταγραφή μία παραβίασης μπορεί να βοηθήσει στην εκτίμηση της ζημιάς.

Κατά τη διάρκεια των αρχικών σταδίων μίας παραβίασης, συχνά δεν είναι πρακτικό να καθοριστεί αν θα γίνει μήνυση, έτσι θα πρέπει να καταγράφονται και να συγκεντρώνονται οποιαδήποτε στοιχεία μπορούν μελλοντικά να φανούν χρήσιμα. Θα πρέπει να γίνει καταγραφή για:

- όλα τα γεγονότα (events) του συστήματος,
- όλες τις ενέργειες που έγιναν,
- όλες τις εξωτερικές συνομιλίες (περιλαμβάνοντας το άτομο με το οποίο έγινε η συνομιλία, την ημερομηνία, την ώρα και το περιεχόμενο της συνομιλίας).

Ο καλύτερος τρόπος για την καταγραφή των στοιχείων είναι η τήρηση ενός ημερολογίου. Αυτό επιτρέπει την καλή αρχειοθέτηση της πληροφορίας μας. Πολλές από αυτές τις πληροφορίες μπορούν να χρησιμοποιηθούν σε ένα δικαστήριο.

Αν είναι εφικτό θα πρέπει να ακολουθηθούν τα παρακάτω βήματα:

- τακτικά (π.χ. κάθε μέρα) να παραδίδουμε επικυρωμένα αντίγραφα του ημερολογίου σε ένα άτομο που θα έχει οριστεί σαν επιβλέπων.
- ο επιβλέπων θα πρέπει να αποθηκεύει αυτές τις φωτοτυπημένες σελίδες σε ένα ασφαλές μέρος (π.χ. ένα χρηματοκιβώτιο).
- κατά την παράδοση της πληροφορίας για φύλαξη, θα πρέπει να επιστρέφεται μία υπογεγραμμένη απόδειξη από τον επιστάτη όπου θα αναφέρεται η παραλαβή και η ημερομηνία παραλαβής.

Πιθανό λάθος κατά την τήρηση αυτών των διαδικασιών μπορεί να καταλήξει σε ακύρωση κάθε στοιχείου που θα παραδοθεί σε ένα δικαστήριο.

4.5.2.3 ΛΗΨΗ ΜΕΤΡΩΝ ΠΕΡΙΟΡΙΣΜΟΥ ΤΩΝ ΖΗΜΙΩΝ

Ο σκοπός της λήψης μέτρων είναι ο περιορισμός της έκτασης μίας επίθεσης. Ένα σημαντικό μέρος του αφορά τη λήψη αποφάσεων (π.χ. καθορισμός για το αν θα γίνει τερματισμός του συστήματος, ή αποσύνδεση από το δίκτυο, αν θα παρακολουθείται η δραστηριότητα του συστήματος ή του δικτύου, αν θα απενεργοποιηθούν λειτουργίες του, όπως μεταφορά απομακρυσμένου αρχείου, κ.λπ.)

Ορισμένες φορές αυτή η απόφαση είναι τετριμμένη. Αν η πληροφορία είναι ομαδοποιημένη, ευπαθής ή ιδιόκτητη θα πρέπει να γίνεται τερματισμός του συστήματος. Πρέπει να λαμβάνεται υπόψη ότι η άρνηση πρόσβασης σε όλους τους χρήστες όταν μία παραβίαση βρίσκεται σε εξέλιξη ειδοποιεί όλους τους χρήστες, συμπεριλαμβανομένων και των χρηστών που έχουν το υποτιθέμενο πρόβλημα, ότι οι διαχειριστές είναι ενήμεροι του

προβλήματος. Αυτό μπορεί να έχει επιβλαβείς επιδράσεις στην έρευνα. Σε ορισμένες περιπτώσεις, είναι συνετή η αφαίρεση όλων των προσβάσεων, και κατόπιν η αποκατάσταση της κανονικής λειτουργίας σε περιορισμένα στάδια. Σε άλλες περιπτώσεις, αξίζει να προκληθεί κάποια ζημιά στο σύστημα αν αυτό έχει σαν αποτέλεσμα την εύρεση του εισβολέα.

Αυτό το στάδιο περιλαμβάνει την εκτέλεση προκαθορισμένων διαδικασιών. Ο οργανισμός ή ο δικτυακός τόπος θα πρέπει εκ των προτέρων να έχουν ορίσει τα αποδεκτά ρίσκα για την περίπτωση που πραγματοποιηθεί μία παραβίαση και θα υπαγορεύουν συγκεκριμένες ενέργειες. Αυτό είναι πολύ σημαντικό όταν χρειάζεται μία γρήγορη απόφαση και δεν είναι δυνατή η επαφή με όλα τα εμπλεκόμενα άτομα προκειμένου να ληφθεί η απόφαση αυτή. Κατά την απουσία προκαθορισμένων διαδικασιών, το άτομο που είναι υπεύθυνο για την παραβίαση, συχνά δεν έχει τη δύναμη να πάρει δύσκολες διαχειριστικές αποφάσεις. Μία τελευταία ενέργεια που θα συμβεί κατά τη διάρκεια του σταδίου αντιμετώπισης της παραβίασης, είναι να ειδοποιηθούν οι αρμόδιες αρχές.

4.5.2.4 ΑΠΑΛΛΑΓΗ

Η κατάλληλη στιγμή για την απαλλαγή από τα κατάλοιπα μιας παραβίασης είναι όταν αυτή προσδιοριστεί με ακρίβεια. Πριν από την εξάλειψη μιας αιτίας, πρέπει να δοθεί μεγάλη προσοχή στη συγκέντρωση όλης της απαραίτητης πληροφορίας για το εκτεθειμένο σύστημα καθώς και την αιτία της παραβίασης, η οποία είναι πολύ πιθανόν να χαθεί κατά τον καθαρισμό του συστήματος.

Υπάρχει διαθέσιμο λογισμικό για να μας βοηθήσει στη διεργασία εξυγίανσης του συστήματος, όπως προγράμματα anti-virus. Αν έχουν δημιουργηθεί «πλαστά» (bogus) αρχεία, προτού σβηστούν θα πρέπει να αρχειοθετηθούν. Στην περίπτωση προσβολής από ιό, είναι πολύ σημαντικός ο καθαρισμός και η αναδιάταξη όλων των μέσων που περιέχουν προσβεβλημένα αρχεία. Τέλος, θα πρέπει να βεβαιώνεται η καλή κατάσταση των αντιγράφων ασφαλείας. Πολλά συστήματα που έχουν προσβληθεί από ιούς, περιοδικά προσβάλλονται ξανά επειδή απλά οι άνθρωποι δεν απομακρύνουν συστηματικά τους ιούς από τα αντίγραφα ασφαλείας. Μετά από την απομάκρυνση πρέπει να ληφθεί ένα νέο αντίγραφο ασφαλείας.

Η εξάλειψη όλων των ευάλωτων σημείων μετά από μια παραβίαση είναι σχεδόν αδύνατη.

Ίσως είναι απαραίτητη η επιστροφή στο αρχικό σύστημα διανομής και η επαναφορά του συστήματος από την αρχή. Για να γίνει αυτό θα πρέπει να διατηρούνται μια εγγραφή αρχικοποίησης του γνήσιου συστήματος και κάθε αλλαγή προσαρμογής (customization change). Στην περίπτωση επίθεσης βασισμένης στο δίκτυο, είναι πολύ σημαντική η εγκατάσταση patches.

Όπως έχει ήδη αναφερθεί ένα security log μπορεί να είναι πιο σημαντικό κατά τη διάρκεια της φάσης απάλειψης των τρωτών σημείων του συστήματος. Τα logs που δείχνουν πως ανακαλύφθηκε και ελέγχθηκε μία παραβίαση μπορούν να χρησιμοποιηθούν αργότερα για να βοηθήσουν στον καθορισμό του μεγέθους της ζημίας. Ιδανικά, κάποιος θα αυτοματοποιούσε και θα εφάρμοζε το ίδιο test με αυτό που χρησιμοποίησε για να ανιχνεύσει την παραβίαση ασφαλείας.

4.5.2.5 ΑΝΑΚΑΜΨΗ ΛΕΙΤΟΥΡΓΙΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ

Όταν έχει εξυγιανθεί η αιτία μίας παραβίασης, το επόμενο στάδιο είναι η φάση της ανάκαμψης των συστημάτων. Ο στόχος της ανάκαμψης είναι η επιστροφή του συστήματος στην αρχική του κατάσταση. Αυτό θα πρέπει να γίνει ενοχλώντας τους χρήστες το λιγότερο δυνατό.

4.5.2.6 ΣΥΝΕΧΗΣ ΕΝΗΜΕΡΩΣΗ (FOLLOW-UP)

Από τη στιγμή που το σύστημα έχει επιστρέψει σε μία σταθερή κατάσταση, είναι πολύ πιθανόν να υπάρχουν «τρύπες» που να απειλούν το σύστημα. Στο σημείο αυτό θα πρέπει να γίνει έλεγχος του συστήματος για πιθανή απώλεια δεδομένων κατά το στάδιο του καθαρισμού του συστήματος.

Το πιο σημαντικό στοιχείο της συνεχής ενημέρωσης είναι να γίνει μία ανάλυση που θα ακολουθεί το γεγονότα. Τι έγινε ακριβώς και ποιες στιγμές; Πόσο καλά αντέδρασαν τα στελέχη στην παραβίαση; Τι είδους πληροφορία χρειάζεται αμέσως το προσωπικό και πως θα μπορούσαν να την πάρουν όσο πιο γρήγορα γίνεται; Τι θα πρέπει να γίνει με διαφορετικό τρόπο την επόμενη φορά;

Μετά την παραβίαση, είναι σκόπιμη η συγγραφή μιας αναφοράς στην οποία θα περιγράφεται η ακριβής ακολουθία των γεγονότων, η μέθοδος ανακάλυψης, η διαδικασία διόρθωσης, η διαδικασία παρακολούθησης και τέλος μία γενική περίληψη. Αυτό θα βοηθήσει στην απόλυτη κατανόηση του προβλήματος.

Μία αναφορά ενημέρωσης είναι πολύτιμη για την αντιμετώπιση άλλων παρόμοιων παραβιάσεων. Είναι επίσης σημαντικό, το συντομότερο δυνατό να αποκτήσουμε μία οικονομική εκτίμηση της ζημιάς που προκάλεσε η παραβίαση. Αυτή η εκτίμηση θα περιλαμβάνει έξοδα που σχετίζονται με κάθε απώλεια σε λογισμικό και αρχεία δεδομένων, τη ζημιά του υλικού, καθώς και έξοδα σε ανθρώπινο δυναμικό που χρησιμοποιήθηκε για την επαναφορά των αρχείων που είχαν αλλοιωθεί. Μια τέτοια εκτίμηση μπορεί να αποτελέσει τη βάση για περαιτέρω ενέργειες δίωξης-μήνυσης. Η αναφορά επίσης μπορεί να βοηθήσει για να αιτιολογηθεί η προσπάθεια ασφάλειας των υπολογιστών ενός οργανισμού στη διαχείριση του οργανισμού.

4.5.2.7 ΕΝΕΡΓΕΙΕΣ ΜΕΤΑ ΤΗΝ ΕΠΙΘΕΣΗ

Ακριβώς μετά την παραβίαση διάφορες ενέργειες θα πρέπει να λάβουν χώρα:

- Πρέπει να κρατηθεί ένας κατάλογος απογραφής των πόρων του συστήματος (π.χ. μία προσεκτική εξέταση θα καθορίσει πως προσβλήθηκε το σύστημα).
- Τα αποτέλεσμα ενός περιστατικού πρέπει θεωρηθούν πηγή μάθησης και να συμπεριληφθούν στο αναθεωρημένο σχέδιο ασφαλείας για να αποτραπεί η επανεμφάνιση του φαινομένου.
- Μία νέα ανάλυση ρίσκου πρέπει να αναπτυχθεί.

Όταν ένας ιστότοπος έχει συνέλθει από μία παραβίαση, η πολιτική και οι διαδικασίες πρέπει να αναθεωρηθούν και να περικλείσουν αλλαγές έτσι ώστε να αποφευχθούν παρόμοια

περιστατικά. Ακόμα και χωρίς κάποια παραβίαση, είναι φρόνιμο να αναθεωρούνται πολιτικές και διαδικασίες σε τακτική βάση. Οι αναθεωρήσεις επιβάλλονται εξαιτίας των σημερινών υπολογιστικών περιβαλλόντων που συνεχώς αλλάζουν.

Ο απώτερος σκοπός της διαδικασίας που ακολουθεί το γεγονός της παραβίασης είναι η βελτίωση των μέτρων ασφαλείας, έτσι ώστε να προστατευθεί ο ιστότοπος από μελλοντικές επιθέσεις. Όσο και να ακούγεται οξύμωρο, ένας οργανισμός ή ένας ιστότοπος έχει, ως αποτέλεσμα μίας παραβίασης, το κέρδος της πρακτικής γνώσης. Ένας πραγματικός στόχος της διαδικασίας που ακολουθεί την παραβίαση είναι η ανάπτυξη μεθόδων για το χρονικό διάστημα πριν τις εκάστοτε επιθέσεις. Μία άλλη σημαντική ενέργεια μετά από ένα τέτοιο συμβάν πρέπει να είναι η εκπαίδευση των χρηστών και του διαχειριστή, ώστε να αποτραπεί η επανεμφάνιση του ίδιου προβλήματος ασφαλείας. Επειδή η πρακτική έχει μεγάλη σημασία, ενδείκνυται να δημιουργούνται εσωτερικά σενάρια επιθέσεων για την εξακρίβωση και βελτίωση της ασφάλειας.

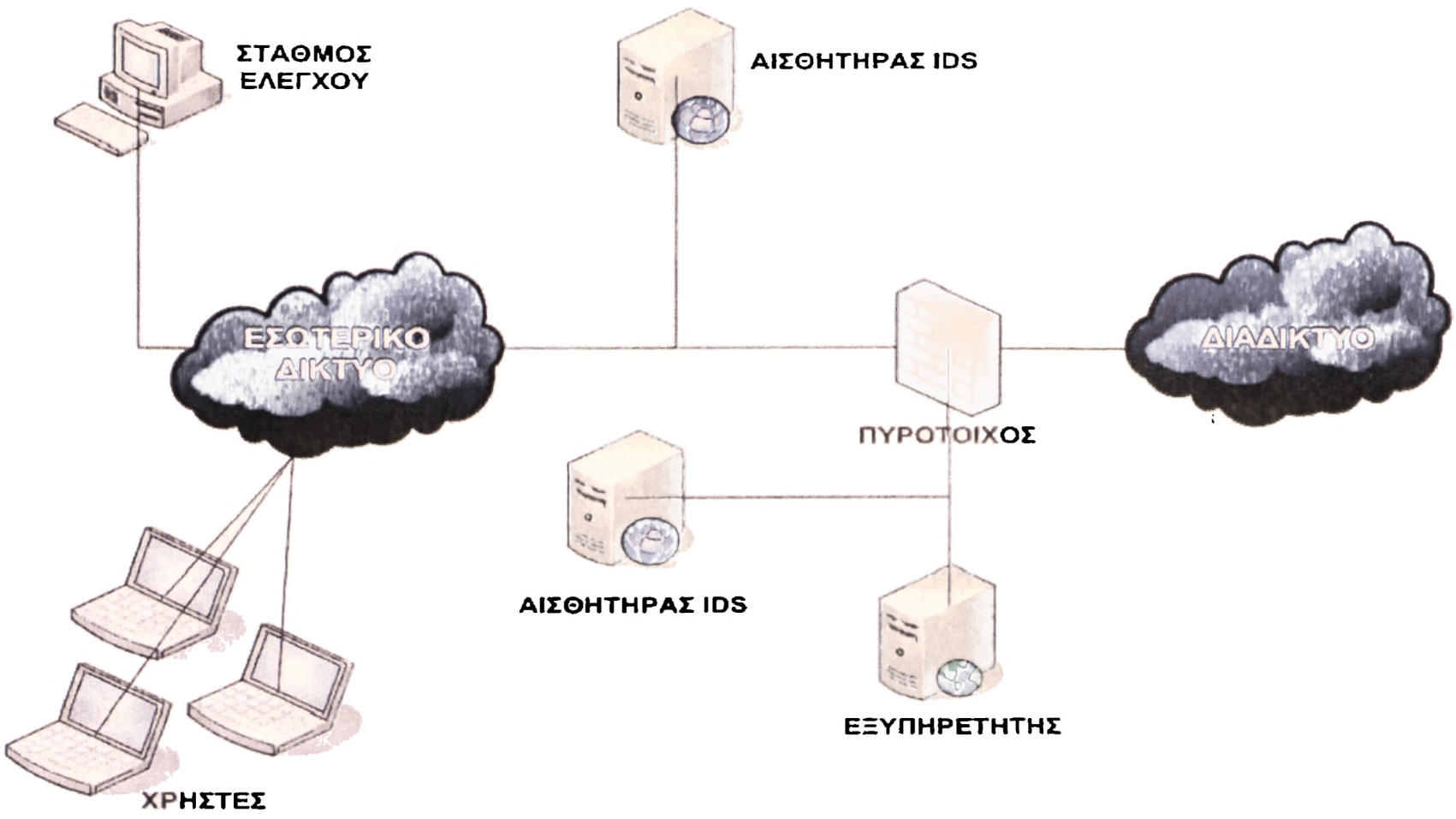
4.6 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (INTRUSION DETECTION SYSTEMS – IDS)

Ένα Σύστημα Ανίχνευσης Επιθέσεων (IDS) εξετάζει τη δραστηριότητα σε ένα σύστημα ή δίκτυο με στόχο να βρει πιθανές εισβολές ή επιθέσεις [NIST 800-31]. Σχεδόν όλα τα Συστήματα Ανίχνευσης Επιθέσεων μέχρι σήμερα χρησιμοποιούν είτε κεντρική ανάλυση δεδομένων, δηλαδή ένα σύστημα συλλέγει πληροφορίες για το δίκτυο συνεχώς και προσπαθεί να αποφανθεί για το αν το δίκτυο είναι υπό επίθεση ή όχι, είτε host-based ανάλυση, δηλαδή στον υπολογιστή του δικτύου συλλέγονται και επεξεργάζονται πληροφορίες για να αποφασίσει το σύστημα αν βρίσκεται υπό επίθεση.

Τα IDS βασίζονται σε δύο τεχνολογίες: Τα **Δικτυακά Συστήματα Ανίχνευσης Επιθέσεων** (Network-Based IDS) και τα **Συστήματα Ανίχνευσης Επιθέσεων Εγκατεστημένα σε υπολογιστές** (Host-Based IDS). Τα δικτυακά συστήματα ανίχνευσης επιθέσεων είναι τα πιο διαδεδομένα και εξετάζουν την διερχόμενη δικτυακή κίνηση (traffic) για ίχνη εισβολής.

Δικτυακά Συστήματα Ανίχνευσης Επιθέσεων (Network-Based IDS)

Το δικτυακό IDS συνήθως αποτελείται από δύο μέρη: τους αισθητήρες και τον σταθμό διαχείρισης/ανάλυσης. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος. Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα, δηλαδή λαμβάνουν όλη την δικτυακή κίνηση, όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και τη διερχόμενη από αυτούς κυκλοφορία με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στον σταθμό διαχείρισης/ανάλυσης. Ο σταθμός διαχείρισης/ανάλυσης μπορεί να δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες ή να πραγματοποιήσει επιπλέον ανάλυση. Το παρακάτω σχήμα (σχήμα 4-3) δείχνει τη διάταξη ενός παραδοσιακού δικτυακού συστήματος ανίχνευσης επιθέσεων με δύο αισθητήρες σε ξεχωριστά δικτυακά τμήματα που επικοινωνούν με ένα σταθμό παρακολούθησης δεδομένων στο εσωτερικό δίκτυο.



Σχήμα 4-3: Διάταξη Δικτυακού IDS

Συστήματα Ανίχνευσης Επιθέσεων εγκατεστημένα σε υπολογιστές (host-based IDS)

Τα συστήματα που είναι host based ψάχνουν για ίχνη εισβολής στο τοπικό σύστημα του host. Χρησιμοποιούν συχνά το μηχανισμό ελέγχου και καταγραφής του host σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό υπολογιστή, όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος. Η συγκεκριμένη αρχιτεκτονική χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας. Για παράδειγμα, ένας τέτοιος κανόνας μπορεί να είναι ο εξής: δυνατότητα για πρόσβαση στο λογαριασμό root (διαχειριστή) είναι δυνατή μόνο μέσω της εντολής su. Συνεπώς, επιτυχημένες προσπάθειες πρόσβασης στο λογαριασμό root θα μπορούσαν να θεωρηθούν ως επίθεση.

4.6.1 ΕΠΙΘΥΜΗΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (IDS)

Τα χαρακτηριστικά του ιδανικού Συστήματος Ανίχνευσης Επιθέσεων παρατίθενται παρακάτω:

1. Πρέπει να τρέχει συνεχώς με ελάχιστη ανθρώπινη παρακολούθηση
2. Πρέπει να μπορεί να αντιμετωπίσει σφάλματα που μπορεί να συμβούν

- Το σύστημα πρέπει να μπορεί να επανέλθει από αποτυχίες του συστήματος, είτε προέρχονται από λάθος είτε σκόπιμες.
- Μετά από μια τέτοια αποτυχία πρέπει να μπορεί να επανέλθει ακριβώς στην προηγούμενη κατάσταση του σαν να μην είχε συμβεί τίποτε.

3. Πρέπει να μην μπορεί να «καταστραφεί»
   - Πρέπει να είναι σχεδόν αδύνατο να τροποποιήσει ή να αχρηστεύσει κάποιος το Σύστημα Ανίχνευσης Επιθέσεων.
   - Πρέπει να υπάρχει τρόπος το Σύστημα να ελέγχει τον εαυτό του και να μπορεί να ανιχνεύσει αν είναι αυτό που δέχτηκε επίθεση.

4. Πρέπει να επηρεάζει ελάχιστα την απόδοση των υπολογιστών στα οποία τρέχει, ώστε να μην παρεμποδίζει την κανονική τους λειτουργία(εκτός αν είναι αποκλειστικά για το Σύστημα Ανίχνευσης Επιθέσεων).
5. Πρέπει να είναι διαμορφώσιμο ώστε να προσαρμόζεται με ακρίβεια στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
6. Πρέπει να είναι ανεξάρτητο λειτουργικού συστήματος, δηλαδή πρέπει να υπάρχει τρόπος να λειτουργήσει για ανίχνευση επίθεσης σε οποιοδήποτε λειτουργικό σύστημα
7. Πρέπει να μπορεί να προσαρμοστεί σε αλλαγές στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
8. Πρέπει να μπορεί να ανιχνεύσει επιθέσεις

   - δεν πρέπει να χαρακτηρίζει σαν επίθεση περιπτώσεις καλής λειτουργίας του δικτύου (false positive).
   - δεν πρέπει να αποτυγχάνει στην ανίχνευση οποιασδήποτε επίθεσης. Πρέπει να είναι πολύ δύσκολο για τον εισβολέα να «καμουφλαριστεί» έτσι ώστε να μην γίνει αντιληπτός σαν εισβολέας από το σύστημα.
   - πρέπει να ανιχνεύει και να αναφέρει τις επιθέσεις όσο πιο γρήγορα γίνεται.
   - πρέπει να είναι αρκετά γενικό ώστε να ανιχνεύει πολλούς διαφορετικούς τύπους επιθέσεων, ακόμα και άγνωστους τύπους επιθέσεων.

4.7 ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΚΑΤΑΣΤΡΟΦΗΣ (DISASTER RECOVERY PLAN)

Το σχέδιο αποκατάστασης καταστροφής σχεδιάζεται για να εξασφαλίσει τη συνέχεια των ζωτικής σημασίας επιχειρησιακών διαδικασιών σε περίπτωση που μια καταστροφή προκύψει [Site7]. Αυτό το σχέδιο θα παράσχει μια αποτελεσματική λύση που μπορεί να χρησιμοποιηθεί για να ανακτήσει όλες τις ζωτικής σημασίας επιχειρησιακές διαδικασίες μέσα στο απαραίτητο χρονικό πλαίσιο χρησιμοποιώντας τα ζωτικής σημασίας αρχεία που αποθηκεύονται εκτός δικτυακού τόπου (off-site). Αυτό το σχέδιο είναι ένα από τα διάφορα σχέδια που θα παράσχουν τις διαδικασίες για να χειριστούν τις καταστάσεις έκτακτης ανάγκης. Αυτά τα σχέδια μπορούν να χρησιμοποιηθούν χωριστά αλλά σχεδιάζονται για να υποστηρίξουν το ένα άλλο το άλλο. Το πρώτο σχέδιο είναι το διοικητικό σχέδιο κρίσης. Αυτό το σχέδιο επιτρέπει τη δυνατότητα να αντιμετωπιστούν οι υψηλού επιπέδου δραστηριότητες συντονισμού που περιβάλλουν οποιαδήποτε κατάσταση κρίσης.

Το επόμενο βασικό ζήτημα που εξετάζεται έντονα μέσα στη στρατηγική για την αποκατάσταση καταστροφής είναι μια στρατηγική αποκατάστασης για εναλλακτική επεξεργασία (Hot-Site). Το σχέδιο αυτό προσδιορίζει τα Hot-Site και τις εναλλακτικές λύσεις εάν η αρχική τοποθεσία δεν είναι διαθέσιμη για να παρέχει τις υπηρεσίες αποκατάστασης καταστροφής για τα διάφορα περιβάλλοντα συστημάτων.

Το τελικό ζήτημα που αντιμετωπίζεται μέσα στη στρατηγική αποκατάστασης καταστροφής είναι να διασφαλιστεί ότι κάθε λογικό μέτρο έχει ληφθεί για να προσδιορίσει και να μετριάσει τους πιθανούς κινδύνους που υπάρχουν μέσα στο περιβάλλον επεξεργασίας. ***Η επιτυχέστερη στρατηγική αποκατάστασης καταστροφής είναι αυτή που δεν θα εφαρμοστεί ποτέ, επομένως η αποφυγή κινδύνου είναι ένα κρίσιμο στοιχείο στη διαδικασία ανάκαμψης καταστροφής.***

4.7.1 ΔΙΟΙΚΗΤΙΚΟ ΣΧΕΔΙΟ ΚΡΙΣΗΣ

Το διοικητικό σχέδιο κρίσης σχεδιάζεται για να εξασφαλίσει τη συνέχεια των ζωτικής σημασίας επιχειρησιακών διαδικασιών σε περίπτωση που εμφανιστεί μια κατάσταση έκτακτης ανάγκης ή κρίσης. Εντούτοις, διοικητικοί υψηλού βαθμού και ο ανώτερος διαχειριστής μπορούν να χρησιμοποιήσουν τις διαδικασίες σε αυτό το σχέδιο. Εάν εμφανιζόταν μια κατάσταση έκτακτης ανάγκης σε οποιεσδήποτε από τις επιχειρησιακές θέσεις, το σχέδιο πρέπει να παράσχει μια αποτελεσματική μέθοδο που μπορεί να χρησιμοποιηθεί από το διοικητικό προσωπικό για να ελέγξει όλες τις δραστηριότητες που συνδέονται με μια κατάσταση κρίσης κατά τρόπο δυναμικό και για να ελαττώσει τον πιθανό αρνητικό αντίκτυπο με τα μέσα (media), το κοινό και με τους μετόχους. Αυτό το σχέδιο πρέπει να ενημερώνεται ετησίως και πρέπει πάντα να είναι εύκολα διαθέσιμο στο εξουσιοδοτημένο προσωπικό.

Πεδία και στόχοι του διοικητικού σχεδίου κρίσης

Το σχέδιο πρέπει να παρέχει τις πληροφορίες για το δυναμικό χειρισμό οποιασδήποτε κατάστασης κρίσης και πρέπει να περιλάβει λεπτομερείς διαδικασίες για τα εξής:

- . Ανώτεροι υπάλληλοι
- . Νομικός
- . Σχέσεις επενδυτών
- . Εταιρικές επικοινωνίες
- . Εταιρική διοίκηση
- . Μάρκετινγκ και πωλήσεις
- . Ανθρώπινο δυναμικό
- . Διαχείριση τεχνολογίας

Το σχέδιο πρέπει επίσης να τεκμηριώσει τις ευθύνες, τις διαδικασίες, και τους πίνακες ελέγχου που θα χρησιμοποιηθούν για να διαχειριστούν και να ελέγξουν την κατάσταση μετά από ένα περιστατικό έκτακτης ανάγκης ή κρίσης.

Το διοικητικό σχέδιο κρίσης έχει αναπτυχθεί για να ολοκληρώσει τους ακόλουθους στόχους:

- Προετοιμασία του ανώτερου διοικητικού προσωπικού για να αποκριθεί αποτελεσματικά σε μια κατάσταση κρίσης
- Διαχείριση της κρίσης με έναν οργανωμένο και αποτελεσματικό τρόπο
- Περιορισμός του μεγέθους ή του αντίκτυπου οποιασδήποτε κατάστασης κρίσης στις διάφορες επιχειρησιακές μονάδες.

Οι δραστηριότητες των διοικητικών σχεδίων κρίσης αρχίζουν από μια διαδικασία κατάστασης ή προειδοποίησης κρίσης. Μετά από την ανακάλυψη ενός περιστατικού, η διοικητική ομάδα κρίσης θα εκτελέσει μια αξιολόγηση της κατάστασης και θα καθορίσει εάν υπάρχει ανάγκη να δηλωθεί μια έκτακτη ανάγκη ή μια κρίση και να ενεργοποιηθεί το διοικητικό σχέδιο κρίσης. Όταν το σχέδιο ενεργοποιείται, το διορισμένο διοικητικό προσωπικό θα προειδοποιηθεί και θα κατευθυνθεί για να ενεργοποιήσει τις διαδικασίες του σχεδίου.

4.7.2 ΣΤΡΑΤΗΓΙΚΗ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

Η στρατηγική αποκατάστασης έχει ως στόχο να εγκαταστήσει τα συστήματα που επεξεργάζονται κρίσιμες πληροφορίες σε έναν εναλλακτικό κέντρο επεξεργασίας.

Φάσεις αποκατάστασης

Οι δραστηριότητες αποκατάστασης θα διευθυνθούν σε μια συγχρονισμένη προσέγγιση. Η έμφαση θα δοθεί στο να ανακτηθούν οι κρίσιμες εφαρμογές αποτελεσματικά και αποδοτικά.

Φάση Ι

Μετακίνηση διαδικασιών στην εφεδρική (Backup) περιοχή αποκατάστασης καταστροφής και το κέντρο διαδικασιών έκτακτης ανάγκης. Αυτή η δραστηριότητα θα αρχίσει με την ενεργοποίηση του σχεδίου αποκατάστασης καταστροφής. Υπάρχει μια περίοδος μέχρι 24 ώρες που επιτρέπει την οργάνωση και τον κύκλο εργασιών της εφεδρικής περιοχής αποκατάστασης καταστροφής.

Φάση ΙΙ

Ανάκτηση των κρίσιμων επιχειρησιακών λειτουργιών, αποκατάσταση των κρίσιμων εφαρμογών και της κρίσιμης συνδεσιμότητας των δικτύων. Ο στόχος εδώ είναι να ανακτηθούν τα συστήματα και το δίκτυο έτσι ώστε οι πελάτες να μπορούν να συνεχίσουν τις επιχειρησιακές δραστηριότητες.

Φάση ΙΙΙ

Επιστροφή των δραστηριοτήτων επεξεργασίας δεδομένων στις αρχικές εγκαταστάσεις ή σε μια άλλη εγκατάσταση υπολογιστών.

4.7.3 ΠΕΔΙΑ ΚΑΙ ΣΤΟΧΟΙ ΤΟΥ ΣΧΕΔΙΟΥ

Το σχέδιο αποκατάστασης καταστροφής παρέχει μια κατάσταση ετοιμότητας που επιτρέπει τη γρήγορη απάντηση του προσωπικού αφότου έχει συμβεί μια καταστροφή. Αυτό, στη συνέχεια, επιτρέπει μια αποτελεσματικότερη και αποδοτική προσπάθεια αποκατάστασης. Το σχέδιο αποκατάστασης καταστροφής πρέπει να αναπτυχθεί για να ολοκληρώσει τους ακόλουθους στόχους [Site7]:

1. Περιορισμός του μεγέθους οποιασδήποτε απώλειας με την ελαχιστοποίηση της διάρκειας μιας κρίσιμης διακοπής υπηρεσιών εφαρμογής.
2. Αξιολόγηση της ζημίας, αποκατάσταση της ζημίας, και ενεργοποίηση του επισκευασμένου κέντρο υπολογιστών.
3. Ανάκτηση των απαραίτητων στοιχείων και πληροφοριών στη λειτουργία της κρίσιμης εφαρμογής.
4. Διαχείριση της λειτουργίας αποκατάστασης με έναν οργανωμένο και αποτελεσματικό τρόπο.
5. Προετοιμασία του προσωπικού τεχνολογίας για να αποκριθεί αποτελεσματικά στις καταστάσεις αποκατάστασης καταστροφής.

Κάθε επιχείρηση έχει την ευθύνη να αποκριθεί σε οποιαδήποτε βραχυπρόθεσμη ή μακροπρόθεσμη διάσπαση των υπηρεσιών. Με την ανάπτυξη, την τεκμηρίωση, την εφαρμογή και τη δοκιμή αυτού του σχεδίου αποκατάστασης καταστροφής, οι επιχειρήσεις θα είναι σε θέση να αποκαταστήσουν τη διαθεσιμότητα των κρίσιμων εφαρμογών κατά τρόπο έγκαιρο και οργανωμένο μετά από ένα περιστατικό καταστροφής. Προκειμένου να ολοκληρωθούν αυτοί οι στόχοι, ο τομέας τεχνολογίας θα εξαρτηθεί από την υποστήριξη της ανώτερης διαχείρισης, τους τελικούς χρήστες και τα τμήματα προσωπικού. Οι δραστηριότητες σχεδίων αποκατάστασης καταστροφής αρχίζουν από μια διαδικασία κατάστασης συναγερμού ή καταστροφής. Μετά από την ανακάλυψη ενός περιστατικού, η διαχείριση τεχνολογίας θα ενημερωθεί για μια πιθανή καταστροφή στο κέντρο υπολογιστών. Η διοικητική ομάδα αποκατάστασης θα εκτελέσει μια αξιολόγηση της κατάστασης και θα καθορίσει εάν υπάρχει μια ανάγκη να δηλωθεί μια καταστροφή και να ενεργοποιηθεί το σχέδιο αποκατάστασης καταστροφής. Όταν το σχέδιο ενεργοποιείται, το προσωπικό ορισμένο για την αποκατάσταση θα προειδοποιηθεί και θα κατευθυνθεί για να ενεργοποιήσει τις διαδικασίες αποκατάστασής τους.

ΚΕΦΑΛΑΙΟ 5ο

5.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

5.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι ένας κλάδος των μαθηματικών που ασχολείται με το μετασχηματισμό των δεδομένων [NIST 800-12]. Η κρυπτογραφία είναι παραδοσιακά συνδεδεμένη με τη μυστικότητα των δεδομένων. Επιπλέον, η σύγχρονη κρυπτογραφία μπορεί να παρέχει πολλές υπηρεσίες στον τομέα της ασφάλειας, όπως για παράδειγμα ηλεκτρονικές υπογραφές, και πιστοποίηση ότι τα δεδομένα δεν έχουν μεταβληθεί. Επίσης, οι σύγχρονες κρυπτογραφικές τεχνικές μπορούν να εξασφαλίζουν την εμπιστευτικότητα (confidentiality) και την ακεραιότητα (integrity) των δεδομένων, ενώ χρησιμοποιούνται σε πολλές προηγμένες τεχνικές πιστοποίησης ταυτότητας.

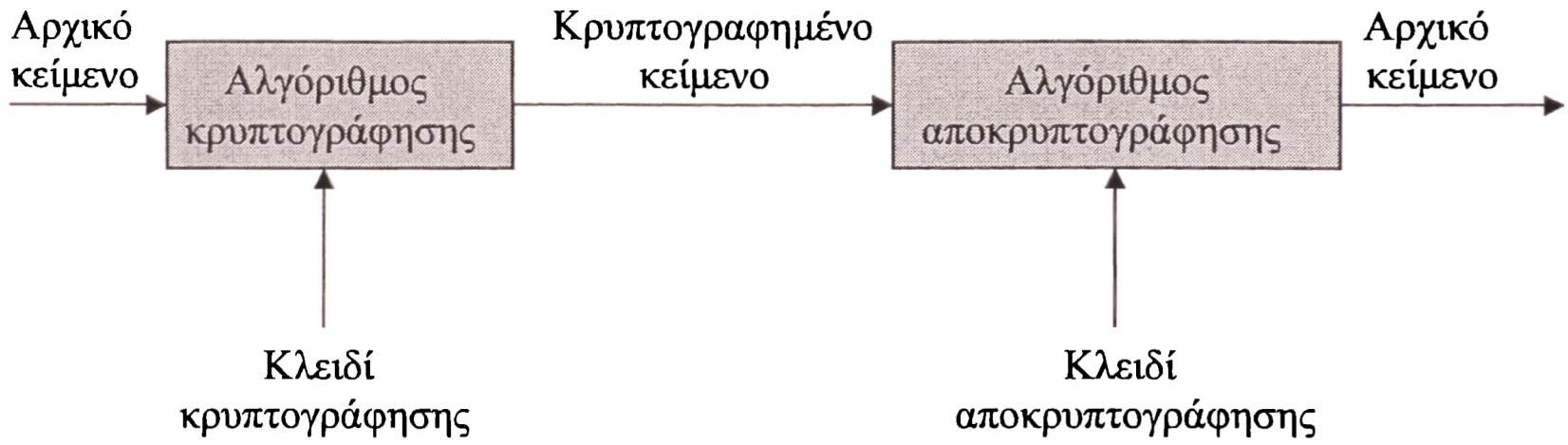
Προσπαθώντας να ορίσουμε την έννοια της κρυπτογραφίας (encryption) μπορούμε να πούμε ότι είναι η διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο από τρίτα μέρη (εκτός του νόμιμου παραλήπτη).

Αποκρυπτογράφηση (decryption) είναι η διεργασία ανάκτησης του αρχικού μηνύματος σε αναγνώσιμη μορφή από μια ακατανόητη έκδοση του που έχει παραχθεί από μια κρυπτογράφηση. Η αποκρυπτογράφηση εκτελείται από κάποιο εξουσιοδοτημένο μέρος, σε αντίθεση με την κρυπτανάλυση που αναλύεται παρακάτω.

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μια διεργασία κρυπτογράφησης, δηλαδή κρυπτογραφείται.

Κρυπτογραφημένο κείμενο (cipher text) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό κείμενο.

Κάθε κρυπτογραφική τεχνική βασίζεται σε δύο συστατικά: έναν αλγόριθμο (ή διαφορετικά μέθοδο κρυπτογράφησης), και το κρυπτογραφικό κλειδί. Στα μοντέρνα κρυπτογραφικά συστήματα, οι αλγόριθμοι είναι σύνθετοι μαθηματικοί τύποι, ενώ τα κλειδιά είναι μεγάλες ακολουθίες από δυαδικά ψηφία. Για να καταστεί δυνατή η κρυπτογραφημένη επικοινωνία δύο μερών, πρέπει αυτά να χρησιμοποιούν τον ίδιο αλγόριθμο, και σε μερικές περιπτώσεις το ίδιο ή συμβατά κρυπτογραφικά κλειδιά. Στο Σχήμα 5-1 φαίνεται η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.



Σχήμα 5-1: Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Η ανθεκτικότητα μιας κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών που χρησιμοποιούνται παρά από τους αλγόριθμους. Το μέγεθος των κλειδιών μετριέται σε bits. Γενικά, μεγάλου μεγέθους κλειδιά παρέχουν ανθεκτικότερη κρυπτογράφηση. Η προσπάθεια να «σπάσει» μια συγκεκριμένη κρυπτογραφική τεχνική

ονομάζεται κρυπτανάλυση. Κρυπτανάλυση είναι η διεργασία αποκρυπτογράφησης ενός μηνύματος από ένα μη εξουσιοδοτημένο άτομο. Τα κρυπτογραφικά συστήματα χρησιμοποιούνται για να παρέχουν:

- μυστικότητα (secrecy)
- ακεραιότητα δεδομένων (data integrity)
- πιστοποίηση χρηστών (user authentication)
- αδυναμία απάρνησης (non-repudiation)

Υπάρχουν δύο βασικοί μέθοδοι στην κρυπτογραφία: τα συστήματα μυστικού κλειδιού (secret key systems), γνωστά και σαν συστήματα συμμετρικών κλειδιών, και τα συστήματα δημόσιου κλειδιού (pubic key systems), γνωστά και σαν συστήματα μη-συμμετρικών κλειδιών. Μια σύγκριση των δύο βασικών αυτών μεθόδων φαίνεται στον πίνακα 5-A [NIST 800-12]. Επίσης υπάρχουν και υβριδικά συστήματα, που στοχεύουν στο συνδυασμό των πλεονεκτημάτων τόσο των συστημάτων μυστικού κλειδιού όσο και αυτών δημόσιου κλειδιού.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	ΚΡΥΠΤΟΓΡΑΦΙΑ ΜΥΣΤΙΚΟΥ ΚΛΕΙΔΙΟΥ	ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ
ΑΡΙΘΜΟΣ ΚΛΕΙΔΙΩΝ	Ένα κλειδί.	Ζεύγος κλειδιών.
ΤΥΠΟΣ ΚΛΕΙΔΙΩΝ	Το κλειδί είναι μυστικό.	Το ένα κλειδί είναι μυστικό και το άλλο δημόσιο.
ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΚΛΕΙΔΙΩΝ	Αποκάλυψη και τροποποίηση.	Αποκάλυψη και τροποποίηση για τα ιδιωτικά κλειδιά και τροποποίηση για τα δημόσια κλειδιά.
ΣΥΓΚΡΙΤΙΚΗ ΤΑΧΥΤΗΤΑ	Πιο γρήγορος.	Πιο αργός.

Πίνακας 5-A: Σύγκριση μεταξύ κρυπτογραφίας μυστικού και δημοσίου κλειδιού

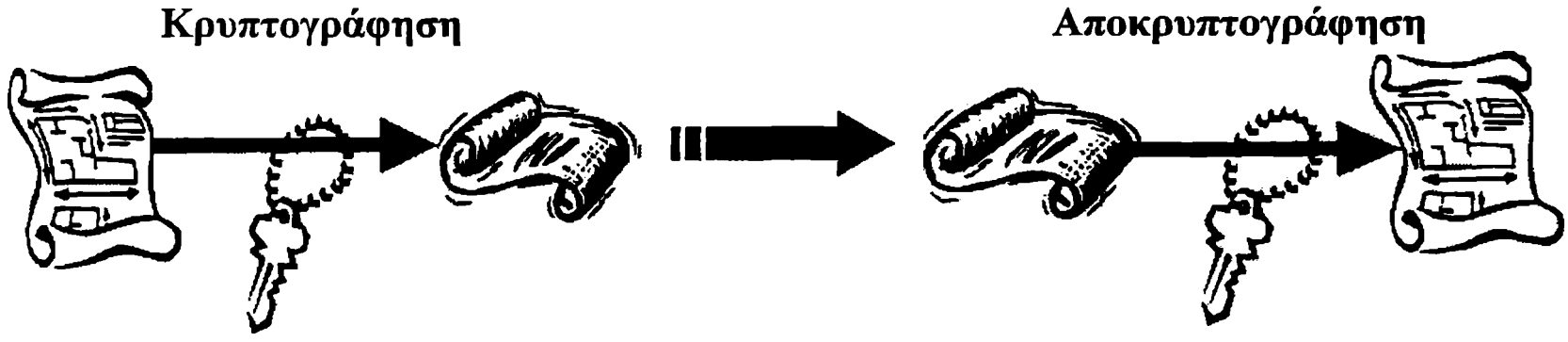
5.1.1 ΣΥΣΤΗΜΑΤΑ ΜΥΣΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

Στα συστήματα μυστικού κλειδιού χρησιμοποιείται ένα μόνο κρυπτογραφικό κλειδί, το οποίο παραμένει μυστικό, και πρέπει να προστατεύεται από υποκλοπή ή μεταβολή. Το σημαντικότερο πλεονέκτημα αυτών των συστημάτων είναι η ταχύτητα τους σε σχέση με τα συστήματα δημόσιου κλειδιού.

Κατά τη διάρκεια της κρυπτογραφημένης επικοινωνίας με σύστημα μυστικού κλειδιού, το ίδιο κρυπτογραφικό κλειδί χρησιμοποιείται τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση των δεδομένων. Η προστασία των δεδομένων βασίζεται αποκλειστικά στην υπόθεση ότι το κλειδί είναι γνωστό μόνο στα μέρη που επικοινωνούν μεταξύ τους, και σε κανέναν τρίτο (Σχήμα 5-2).

Το πιο γνωστό πρότυπο συστήματος μυστικού κλειδιού είναι το DES (Data Encryption Standard), το οποίο δημοσιεύτηκε από το NIST (National Institute of Standards and Technology), σαν Federal Information Processing Standard. Αρκετές φορές τα τελευταία χρόνια η ασφάλεια που προσφέρει το DES έχει τεθεί υπό αμφισβήτηση. Παρόλα αυτά, μέχρι στιγμής δεν έχει αποδειχθεί ότι το DES δεν προσφέρει ισχυρή ασφάλεια και μέχρι σήμερα παραμένει μια από τις ευρύτατα αποδεκτές κρυπτογραφικές μεθόδους η οποία είναι δημόσια διαθέσιμη και μπορεί να χρησιμοποιηθεί από οποιονδήποτε.

Ένα άλλο πρότυπο σύστημα κρυπτογραφίας μυστικού κλειδιού είναι το Escrow Encryption Standard - EES, στο οποίο η φύλαξη των μυστικών κλειδιών αφήνεται σε τρίτους, οι οποίοι παίζουν το ρόλο του εγγυητή. Σε αυτό το πρότυπο λαμβάνεται μέριμνα για ανεπιθύμητες καταστάσεις που μπορούν να διαμορφωθούν από την εξαιρετικά ισχυρή ασφάλεια που οι κρυπτογραφικές τεχνικές προσφέρουν. Σε αυτό το πρότυπο, οι εγγυητές μπορούν να παραχωρήσουν το κρυπτογραφικό κλειδί, όταν οι συνθήκες το επιβάλλουν. Με αυτό τον τρόπο, όταν οι συνθήκες επιβάλλουν την παρακολούθηση της επικοινωνίας δύο μερών (π.χ. παρακολούθηση για λόγους εθνικής ασφάλειας), οι εξουσιοδοτημένοι φορείς (π.χ. εθνική κυβέρνηση, διοίκηση ενός οργανισμού) μπορούν να αποκτήσουν το κλειδί από τους εγγυητές ώστε να διενεργήσουν την παρακολούθηση.



Σχήμα 5-2: Κρυπτογράφηση μυστικού κλειδιού

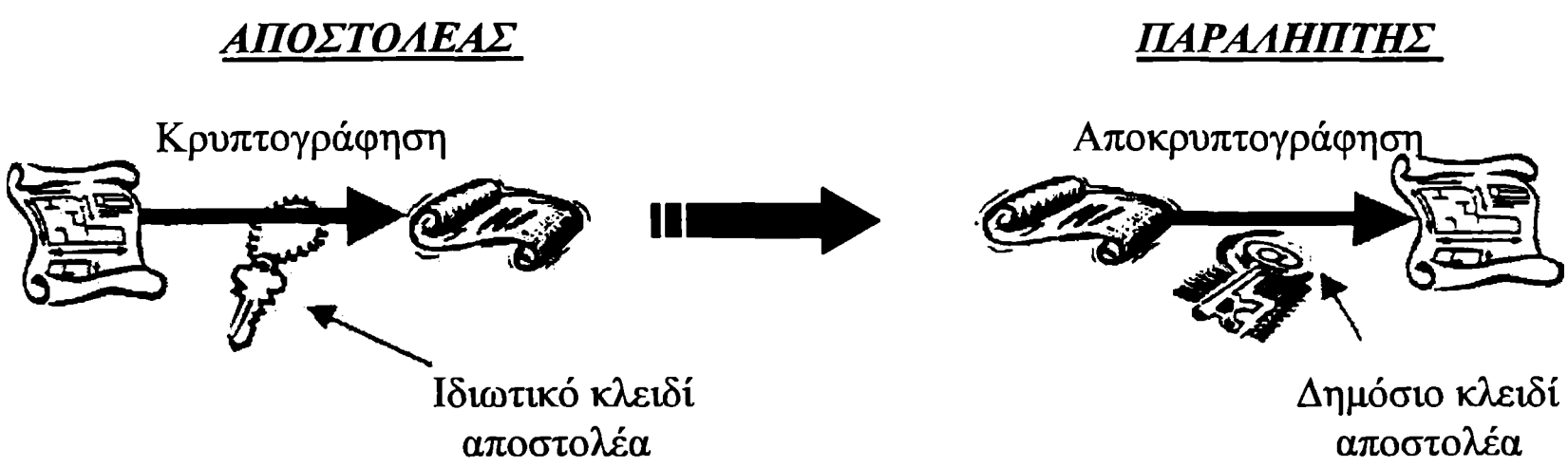
5.1.2 ΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Στα συστήματα δημοσίου κλειδιού κάθε οντότητα χρησιμοποιεί ένα ζευγάρι κρυπτογραφικών κλειδιών, το ένα από αυτά είναι δημόσια γνωστό (δημόσιο κλειδί) ενώ το άλλο είναι μυστικό (ιδιωτικό κλειδί). Σε αυτά τα συστήματα το ιδιωτικό κλειδί πρέπει να προστατεύεται από υποκλοπή ή τροποποίηση, ενώ και το δημόσιο κλειδί πρέπει να προστατεύεται για ενδεχόμενη τροποποίηση.

Τα συστήματα αυτά μπορούν να χρησιμοποιηθούν τόσο για κρυπτογραφημένη επικοινωνία όσο και σαν συστήματα ηλεκτρονικών υπογραφών, αλλά έχουν το μειονέκτημα να είναι πιο αργά από τα συστήματα μυστικού κλειδιού. Το σημαντικότερο πλεονέκτημα των συστημάτων δημοσίου κλειδιού είναι ότι για να επικοινωνήσουν δύο οντότητες δεν χρειάζεται η μία να γνωρίζει το ιδιωτικό κλειδί της άλλης.

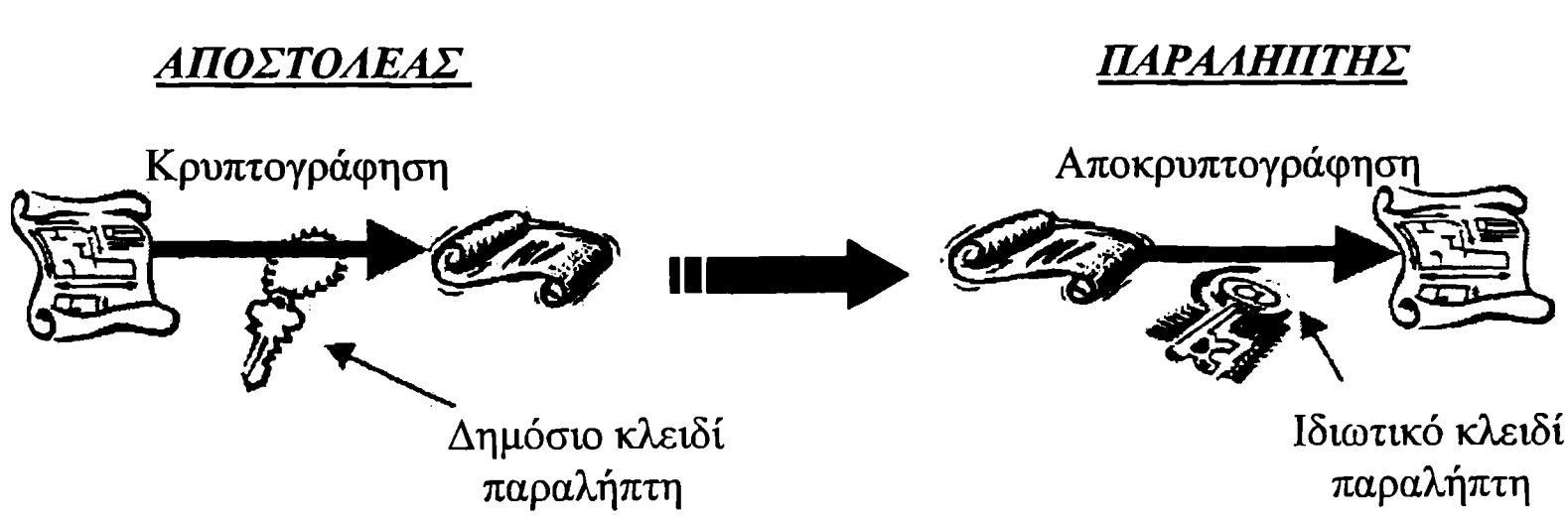
Η διαδικασία κρυπτογράφησης με τη χρήση του παραπάνω ζεύγους κλειδιών μπορεί να γίνει με τρεις τρόπους:

1. Ο αποστολέας μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί ίου για την κρυπτογράφηση της πληροφορίας. Ο παραλήπτης που έχει ήδη διαθέσιμο το δημόσιο κλειδί του αποστολέα μπορεί να αποκρυπτογραφήσει το μήνυμα (Σχήμα 5-3). Με αυτό τον τρόπο μπορεί ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα, αφού μόνο εκείνος γνωρίζει το ιδιωτικό κλειδί που χρησιμοποιήθηκε. Παρόλα αυτά δεν μπορεί να είναι σίγουρος για την εμπιστευτικότητα των δεδομένων, γιατί οποιοσδήποτε θα μπορούσε να χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα και να αποκρυπτογραφήσει το μήνυμα.



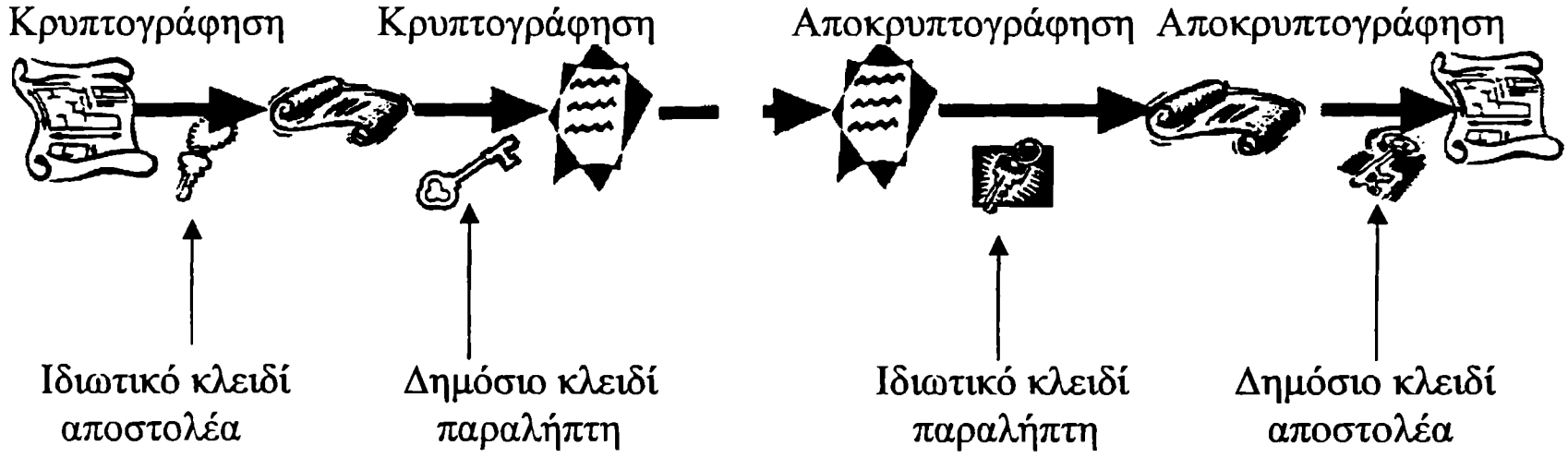
Σχήμα 5-3: *Κρυπτογράφηση δημοσίου κλειδιού (περίπτωση 1η)*

2. Εάν ο αποστολέας χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση τότε μόνο ο παραλήπτης με το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα (Σχήμα 5-4). Αυτή η διαδικασία εξασφαλίζει την εμπιστευτικότητα της πληροφορίας όμως δεν μπορεί να αποκαλύψει την ταυτότητα του αποστολέα αφού οποιοσδήποτε θα μπορούσε να έχει το δημόσιο κλειδί που έκανε την κρυπτογράφηση.



Σχήμα 5-4: Κρυπτογράφηση δημοσίου κλειδιού (περίπτωση 2η)

3. Όταν οι δύο παραπάνω μέθοδοι συνδυαστούν μπορεί να επιτευχθεί τόσο η εμπιστευτικότητα της πληροφορίας όσο και η ταυτοποίηση του αποστολέα. Σύμφωνα με αυτή την προσέγγιση ο αποστολέας μπορεί να κρυπτογραφήσει τα δεδομένα πρώτα με το ιδιωτικό του κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης χρησιμοποιεί το ιδιωτικό του για να το αποκρυπτογραφήσει και στη συνέχεια αποκρυπτογραφεί το αποτέλεσμα με το δημόσιο κλειδί του αποστολέα (Σχήμα 5-5).



Σχήμα 5-5: Κρυπτογράφηση δημοσίου κλειδιού (περίπτωση 3η)

5.1.3 ΥΒΡΙΔΙΚΑ ΣΥΣΤΗΜΑΤΑ

Τόσο τα συστήματα μυστικού όσο και τα συστήματα δημόσιου κλειδιού έχουν συγκριτικά πλεονεκτήματα και μειονεκτήματα. Για παράδειγμα, στα συστήματα δημόσιου κλειδιού η επικοινωνία δεν βασίζεται στη γνώση ενός κοινού, μυστικού κλειδιού. Από την άλλη πλευρά τα συστήματα μυστικού κλειδιού μπορεί να είναι από 1.000 μέχρι 10.000 φορές ταχύτερα από τα αντίστοιχα συστήματα δημόσιου κλειδιού.

Με σκοπό να μεγιστοποιηθούν τα οφέλη από τη χρήση κάθε τεχνικής, μπορούν να χρησιμοποιηθούν υβριδικά συστήματα, τα οποία χρησιμοποιούν και τα δύο είδη κρυπτογραφικών συστημάτων με συμπληρωματικό τρόπο. Με αυτό τον τρόπο τα ταχύτερα συστήματα μυστικού κλειδιού χρησιμοποιούνται για την κρυπτογράφηση σημαντικού όγκου δεδομένων, ενώ τα συστήματα δημόσιου κλειδιού χρησιμοποιούνται για λιγότερο απαιτητικές εφαρμογές. Για παράδειγμα, τα δεδομένα που ανταλλάσσονται κατά τη διάρκεια της επικοινωνίας κρυπτογραφούνται με σύστημα μυστικού κλειδιού, και ένα σύστημα δημόσιου κλειδιού χρησιμοποιείται για την ανταλλαγή του κρυπτογραφικού κλειδιού για την προηγούμενη σύνδεση.

5.1.4 ΧΡΗΣΕΙΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Οι κρυπτογραφικές τεχνικές μπορούν να χρησιμοποιηθούν τόσο για την προστασία των

δεδομένων τόσο κατά την αποθήκευση τους στο εσωτερικό ενός υπολογιστικού συστήματος, όσο και κατά τη μετάδοση τους μεταξύ διαφορετικών υπολογιστικών συστημάτων. Τα δεδομένα που έχουν αποθηκευθεί σε ένα υπολογιστικό σύστημα συνήθως προστατεύονται από τις διαδικασίες ελέγχου πρόσβασης, οπότε οι κρυπτογραφικές τεχνικές παίζουν συμπληρωματικό ρόλο ή χρησιμοποιούνται όταν οι διαδικασίες ελέγχου πρόσβασης δεν μπορεί να είναι πολύ ισχυρές (π.χ. δεδομένα που αποθηκεύονται σε δισκέτες ή σε φορητούς υπολογιστές που μεταφέρονται εκτός οργανισμού). Από την άλλη πλευρά, όταν τα δεδομένα μεταδίδονται σε ένα δίκτυο, τότε η κρυπτογραφία είναι πολλές φορές ο μόνος ασφαλής τρόπος προστασίας από την υποκλοπή. Οι σύγχρονες κρυπτογραφικές τεχνικές μπορούν να προσφέρουν προστασία και ακεραιότητα δεδομένων, καθώς να χρησιμοποιηθούν για συστήματα ηλεκτρονικών υπογραφών και προηγμένα συστήματα πιστοποίησης ταυτότητας.

■ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Ένας από τους πιο ασφαλείς και οικονομικά αποδοτικούς τρόπους να διασφαλιστεί η εμπιστευτικότητα των δεδομένων είναι η κρυπτογράφηση τους. Η διαδικασία κρυπτογράφησης μετατρέπει τα δεδομένα (στην κρυπτογραφική ορολογία plaintext) σε μια κρυπτογραφημένη συμβολοσειρά (cipher text), η οποία δεν παρέχει καμία χρήσιμη πληροφορία και επομένως δεν χρειάζεται να προστατεύεται από την υποκλοπή. Παρόλα αυτά, αν η κρυπτογραφημένη συμβολοσειρά αλλοιωθεί ή τροποποιηθεί δεν θα είναι δυνατή η ορθή αποκωδικοποίηση της. Όλα τα συστήματα μυστικού κλειδιού και τα πιο γνωστά από τα συστήματα δημόσιου κλειδιού μπορούν να χρησιμοποιηθούν για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.

Στα συστήματα μυστικού κλειδιού, τα δεδομένα κρυπτογραφούνται και αποκρυπτογραφούνται με τη χρήση του ίδιου κλειδιού, το οποίο προφανώς πρέπει να είναι μυστικό.

Στην περίπτωση συστημάτων δημόσιου κλειδιού, το μήνυμα κρυπτογραφείται από τον αποστολέα με χρήση του δημόσιου κλειδιού του παραλήπτη, ενώ ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί για την αποκρυπτογράφηση. Με αυτό τον τρόπο, αφού μόνο ο παραλήπτης γνωρίζει το κλειδί της αποκρυπτογράφησης, είναι και ο μοναδικός που μπορεί να αποκρυπτογραφήσει σωστά τα δεδομένα.

■ ΑΚΕΡΑΙΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ

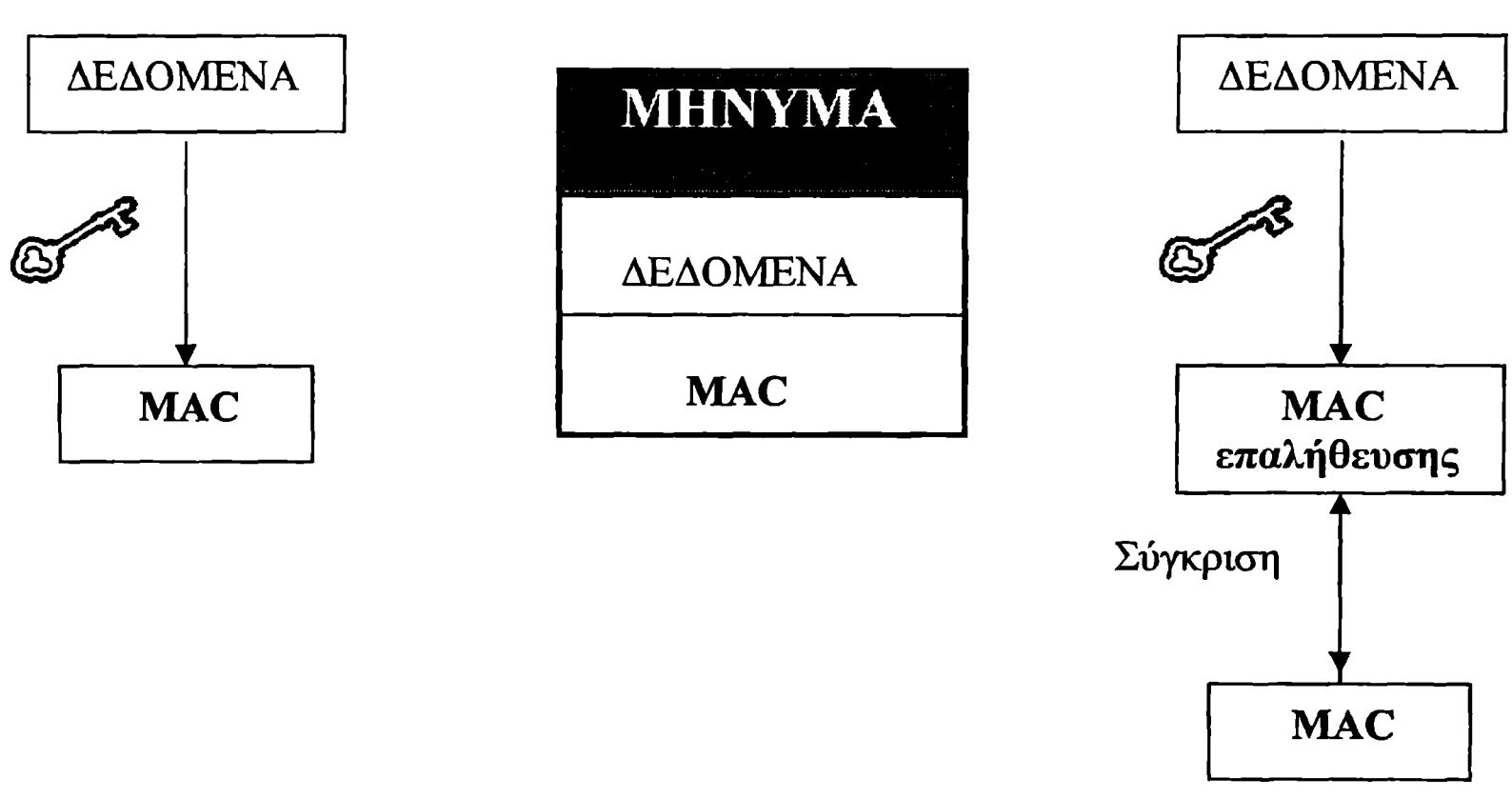
Σε κάθε περίπτωση αποθήκευσης πληροφορίας σε ψηφιακή μορφή, είναι πολύ δύσκολο για κάποιον άνθρωπο να ελέγξει αν η πληροφορία τροποποιήθηκε. Είναι λοιπόν ιδιαίτερα σημαντικό να υπάρχουν μέθοδοι με τη βοήθεια των οποίων θα είναι δυνατός ο έλεγχος για την ακεραιότητα δεδομένων που έχουν αποθηκευθεί σε ένα υπολογιστικό σύστημα.

Μια κατηγορία μεθόδων που μπορούν να χρησιμοποιηθούν για αυτό το σκοπό είναι οι κώδικες ανίχνευσης και διόρθωσης λαθών (π.χ χρήση δυαδικών ψηφίων ισοτιμίας parity bits). Αν και αυτοί οι κώδικες έχουν σημαντική επιτυχία στην ανίχνευση και διόρθωση λαθών που δεν έγιναν σκόπιμα (π.χ. οφείλονται σε λάθη στη γραμμή μετάδοσης), είναι εύκολο να παραπλανηθούν, όταν οι αλλαγές γίνονται με πρόθεση.

Από την άλλη πλευρά, αν και οι κρυπτογραφικές τεχνικές ούτε μπορούν να προφυλάξουν τα δεδομένα από τροποποίηση, ούτε να διορθώσουν λάθη τροποποίησης, παρέχουν σημαντική ασφάλεια στον έλεγχο για την ακεραιότητα των δεδομένων. Τόσο τα

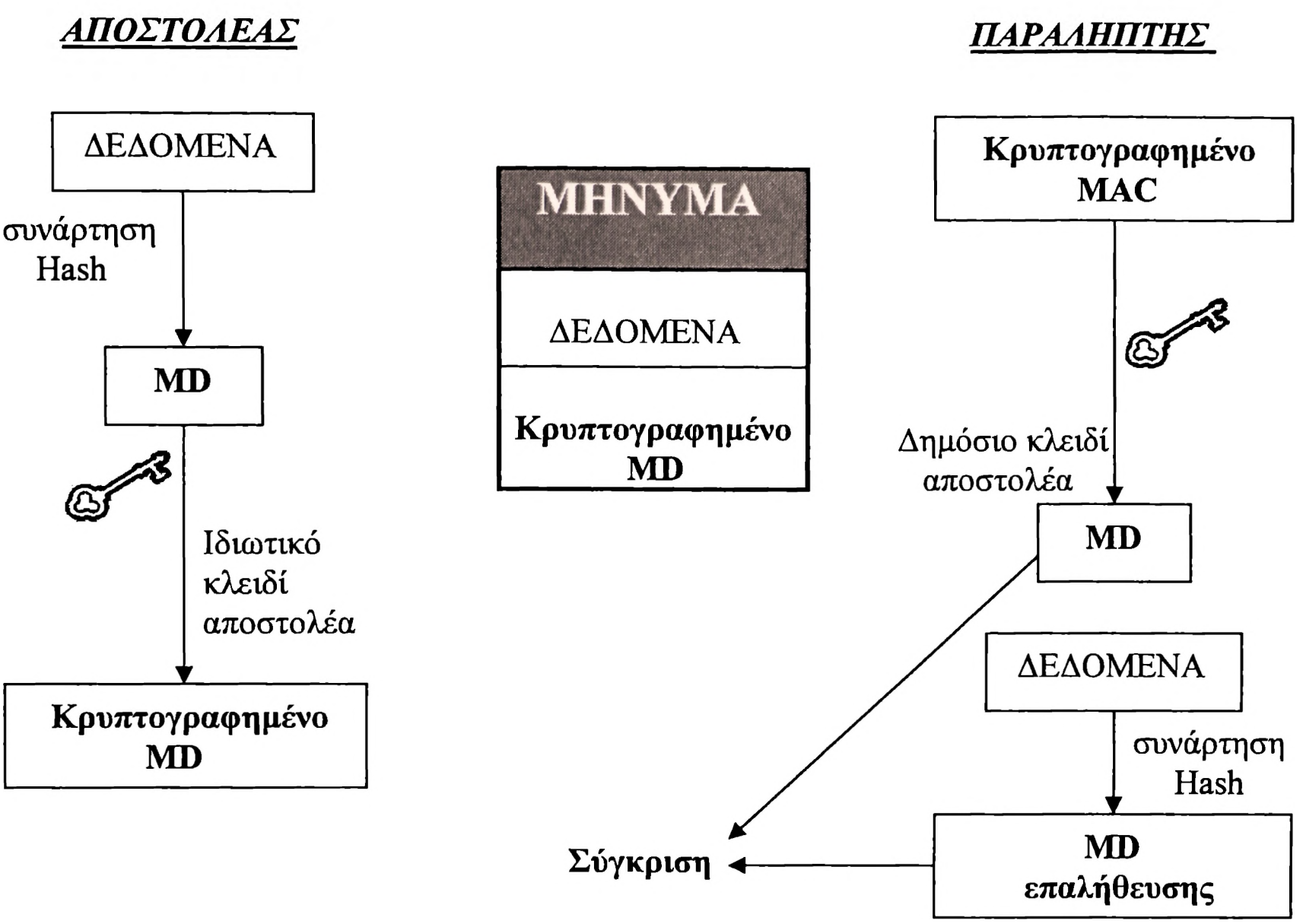
συστήματα μυστικού κλειδιού όσο και τα συστήματα δημόσιου κλειδιού μπορούν να χρησιμοποιηθούν για αυτό το σκοπό.

Στην περίπτωση χρήσης συστήματος μυστικού κλειδιού, ένας Κωδικός Πιστοποίησης Μηνύματος (Message Authentication Code - MAC) υπολογίζεται από τα δεδομένα με χρήση του μυστικού κλειδιού. Αυτός ο κωδικός αποθηκεύεται μαζί με τα δεδομένα, και όποιος γνωρίζει το μυστικό κλειδί μπορεί να τον υπολογίσει εκ νέου, και να τον συγκρίνει με αυτόν που έχει αποθηκευτεί, ώστε να διαπιστώσει αν η πληροφορία έχει τροποποιηθεί (Σχήμα 5-6). Το πρότυπο FIPS 113 με τίτλο Computer Data Authentication καθορίζει μια τυποποιημένη τεχνική για τον υπολογισμό και την αποθήκευση του κωδικού πιστοποίησης μηνύματος.



Σχήμα 5-6: Κωδικός Πιστοποίησης Μηνύματος

Στην περίπτωση χρήσης συστήματος δημόσιου κλειδιού, μια ασφαλής hash συνάρτηση υπολογίζει έναν μικρού μήκους αριθμητικό κωδικό από τα δεδομένα. Αυτός ο κωδικός ονομάζεται και σύνοψη του μηνύματος (message digest) σχήμα 5-7. Η ασφαλής hash συνάρτηση έχει την ιδιότητα ότι δύο διαφορετικά αρχεία είναι απίθανο να έχουν τον ίδιο κωδικό. Αυτός ο κωδικός κρυπτογραφείται με χρήση του ιδιωτικού κλειδιού και αποθηκεύεται μαζί με τα δεδομένα. Ο οποιοσδήποτε μπορεί να αποκρυπτογραφήσει τον κωδικό με χρήση του δημόσιου κλειδιού, καινά τον συγκρίνει με τον κωδικό που αντιστοιχεί στην παρούσα κατάσταση των δεδομένων. Με αυτό τον τρόπο μπορεί εύκολα να διαπιστωθεί η ακεραιότητα των δεδομένων.



Σχήμα 5-7: Σύνοψη Μηνύματος

■ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ

Μια ηλεκτρονική υπογραφή είναι ένας κρυπτογραφικός μηχανισμός που λειτουργεί όπως ακριβώς η γραπτή υπογραφή. Όπως και η γραπτή υπογραφή, η ψηφιακή υπογραφή μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει τον αποστολέα του μηνύματος. Για παράδειγμα, ο παραλήπτης ενός μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να επιβεβαιώσει το πρόσωπο που έχει υπογράψει το μήνυμα, και ότι η πληροφορία του μηνύματος δεν έχει τροποποιηθεί από τη στιγμή που αυτό υπογράφηκε. Επίσης, ο αποστολέας του μηνύματος δεν μπορεί να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα με το συγκεκριμένο περιεχόμενο.

Τα συστήματα ηλεκτρονικών υπογραφών που είναι σήμερα διαθέσιμα βασίζονται σε κρυπτογραφικές τεχνικές, και παρέχουν τουλάχιστον τόση ασφάλεια όσο η γραπτή υπογραφή. Τα συστήματα ηλεκτρονικών υπογραφών βασίζονται στη μυστικότητα των κρυπτογραφικών κλειδιών και στην ανάθεση του κρυπτογραφικού κλειδιού στον κάτοχο του. Αν το κρυπτογραφικό κλειδί υποκλαπεί, τότε ο υποκλοπέας μπορεί να προσποιηθεί ότι είναι ο πραγματικός κάτοχος του κλειδιού. Από την άλλη πλευρά, και η γραπτή υπογραφή μπορεί να πλαστογραφηθεί. Επίσης, είναι προφανές ότι η γραπτή υπογραφή (π.χ σε ψηφιοποιημένη μορφή) δεν μπορεί να χρησιμοποιηθεί για να πιστοποιήσει το συγγραφέα/αποστολέα ενός εγγράφου. Η γραπτή υπογραφή σε τέτοια μορφή μπορεί εύκολα να μεταφερθεί από το ένα έγγραφο στο άλλο παραμένοντας αναλλοίωτη. Τόσο τα κρυπτογραφικά συστήματα μυστικού κλειδιού όσο και αυτά δημόσιου κλειδιού μπορούν να χρησιμοποιηθούν για την υλοποίηση

ψηφιακών υπογραφών. Παρόλα αυτά, τα συστήματα δημόσιου κλειδιού είναι πιο ευέλικτα και πιο κατάλληλα για αυτό το σκοπό.

Στην περίπτωση των συστημάτων μυστικού κλειδιού, οι ηλεκτρονικές υπογραφές μπορούν να υλοποιηθούν με την χρήση του κωδικού πιστοποίησης δεδομένων (MAC). Για παράδειγμα, για ένα ζευγάρι οντοτήτων που επικοινωνεί με χρήση ενός κοινού μυστικού κλειδιού, όταν μία οντότητα λάβει ένα αρχείο που έχει υπογραφεί με έναν κωδικό πιστοποίησης μηνύματος, τότε μπορεί εύκολα να επιβεβαιώσει, με χρήση του κοινού κρυπτογραφικού κλειδιού, ότι το μήνυμα έχει σταλθεί από την άλλη οντότητα, και δεν έχει τροποποιηθεί στη διαδρομή. Αυτή η απλή διαδικασία έχει το μειονέκτημα ότι προϋποθέτει εμπιστοσύνη μεταξύ των δύο οντοτήτων που επικοινωνούν. Πιο προηγμένες τεχνικές μπορούν να χρησιμοποιηθούν για άρση της υπόθεσης για εμπιστοσύνη μεταξύ των δύο οντοτήτων. Αξίζει να σημειωθεί ότι η ομοσπονδιακή κυβέρνηση των Η.Π.Α. έχει ήδη εγκρίνει τη χρήση της τεχνολογίας κωδικού πιστοποίησης μηνύματος σαν εναλλακτικό της γραπτής υπογραφής.

Τα συστήματα δημόσιου κλειδιού είναι τα πλέον κατάλληλα για την υλοποίηση ηλεκτρονικών υπογραφών, που σε αυτή την περίπτωση πολλές φορές ονομάζονται και ψηφιακές υπογραφές (digital signatures). Τα δεδομένα υπογράφονται (κρυπτογραφούνται) με χρήση του ιδιωτικού κλειδιού του αποστολέα. Για να επιταχυνθεί η διαδικασία, συνήθως κρυπτογραφείται μόνο η σύνοψη των δεδομένων (message digest) που αντιστοιχείται στα δεδομένα από μία ασφαλή hash συνάρτηση. Η κρυπτογραφημένη σύνοψη του μηνύματος ονομάζεται ψηφιακή υπογραφή, και αποθηκεύεται ή μεταδίδεται μαζί με τα δεδομένα. Η ταυτότητα του αποστολέα, καθώς και η ακεραιότητα των δεδομένων μπορούν εύκολα να πιστοποιηθούν από οποιονδήποτε, με χρήση του δημόσιου κλειδιού του αποστολέα. Το χαρακτηριστικό αυτό είναι ιδιαίτερα επιθυμητό όταν για παράδειγμα μια εταιρεία προωθεί λογισμικό, το οποίο είναι πιστοποιημένο ότι δεν περιέχει ιούς ή άλλο επιβλαβή κώδικα (malicious code). Η εταιρεία μπορεί να υπογράψει ψηφιακά το μήνυμα, και κάθε παραλήπτης μπορεί να χρησιμοποιήσει το δημόσιο κλειδί της εταιρείας ώστε να επιβεβαιώσει ότι το λογισμικό που παρέλαβε συνεχίζει να είναι αυτό που απέστειλε η εταιρεία, και επομένως μπορεί να εγκατασταθεί άφοβα. Το NIST έχει δημοσιεύσει τις τυποποιήσεις FIPS 186, Digital Signature Standard, και FIPS 180, Secure Hash Standard (SHS), σχετικά με την υλοποίηση ψηφιακών υπογραφών και ασφαλών hash συναρτήσεων.

Επίσης, σε περιβάλλοντα που δεν χρησιμοποιούνται κρυπτογραφικές τεχνικές για υλοποίηση ηλεκτρονικών υπογραφών, υπάρχουν μερικές πρακτικές μέθοδοι, που προσφέρουν ικανοποιητικό βαθμό ασφάλειας, για να διαπιστωθεί η πραγματική ταυτότητα του αποστολέα ενός ηλεκτρονικού μηνύματος.

- Μια απλή μέθοδος συνίσταται στον έλεγχο της διαδρομής του μηνύματος στο δίκτυο. Στα μηνύματα ηλεκτρονικού ταχυδρομείου που διακινούνται στο Διαδίκτυο σημειώνονται ο κόμβος του αποστολέα και η πλήρης διαδρομή του μηνύματος στο δίκτυο

- Όταν δύο μέρη επικοινωνούν μέσω ενός πάροχου δικτυακών υπηρεσιών (π.χ. Internet Service Provider) τότε ο πάροχος μπορεί συνήθως να ελέγξει και να επιβεβαιώσει τον αποστολέα του μηνύματος και την ακεραιότητα των δεδομένων.

- Εφόσον υπάρχει εμπιστοσύνη μεταξύ των οντοτήτων που επικοινωνούν ο παραλήπτης ενός μηνύματος μπορεί εύκολα να επιβεβαιώσει τον αποστολέα και το περιεχόμενο στέλνοντας ένα μήνυμα επιβεβαίωσης.

- Τέλος τα εξερχόμενα μηνύματα και το περιεχόμενο τους πρέπει να καταγράφονται στα αρχεία δραστηριότητας του συστήματος για ενδεχόμενη μελλοντική χρήση.

■ ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ

Η χρήση κρυπτογραφικών τεχνικών μπορεί να βελτιώσει σημαντικά την ασφάλεια των διαδικασιών ταυτοποίησης και πιστοποίησης. Η κρυπτογραφία είναι η βάση για την υλοποίηση αρκετών προηγμένων μεθόδων για πιστοποίηση ταυτότητας, όπως για παράδειγμα του εξυπηρετητή πιστοποίηση Kerberos που προσφέρει εφ' άπας πιστοποίηση, μεθόδων που βασίζονται σε κωδικούς πρόσβασης μιας χρήσης, μεθόδων ερώτησης-απόκρισης (challenge - response) κλπ. Αυτές οι μέθοδοι χρησιμοποιούν διάφορες κρυπτογραφικές τεχνικές και επιτυγχάνουν, ακόμα και αν τα δεδομένα πιστοποίησης υποκλαπούν, να είναι δύσκολο να χρησιμοποιηθούν επιτυχώς από κάποιον επίδοξο εισβολέα.

5.1.5 ΠΟΛΙΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Κρυπτογράφηση θα πρέπει να χρησιμοποιηθεί για την ασφαλή αποθήκευση και μεταφορά των ευαίσθητων και εμπιστευτικών πληροφοριών. Τα κλειδιά κρυπτογράφησης θα πρέπει να αντιμετωπίζονται ως εμπιστευτική πληροφορία. Όλα τα κλειδιά, μυστικά και δημόσια, θα πρέπει να προστατευτούν από την αναρμόδια τροποποίησή τους και από την αναρμόδια κοινοποίησή τους. Η διαχείριση των κλειδιών περιλαμβάνει τις διαδικασίες, χειροκίνητες ή αυτοματοποιημένες και τα πρωτόκολλα που χρησιμοποιούνται κατά τη διάρκεια του κύκλου ζωής των κλειδιών. Ο κύκλος ζωής περιλαμβάνει την παραγωγή, διανομή, αποθήκευση, είσοδος, χρήση, καταστροφή, και αρχειοθέτηση των κρυπτογραφικών κλειδιών. Για τη διανομή των κλειδιών κρυπτογράφησης θα πρέπει να χρησιμοποιηθούν ασφαλή μέσα. Το μήκος των κλειδιών κρυπτογράφησης θα πρέπει να είναι μεγαλύτερο από 56 bits. Τυχόν υποψία κλοπής των κλειδιών κρυπτογράφησης θα πρέπει να αναφέρεται στο διαχειριστή του συστήματος. Όταν απαιτείται επισκευή κάποιου υπολογιστικού συστήματος της επιχείρησης τότε προτού σταλεί προς επισκευή θα πρέπει να κρυπτογραφούνται όλα τα δεδομένα που έχουν αποθηκευτεί στο σκληρό δίσκο. Τα κρυπτογραφικά συστήματα θα πρέπει να σχεδιαστούν έτσι ώστε να απαιτείται η συνεργασία τουλάχιστον δύο ατόμων για την αποκρυπτογράφηση κάποιων ιδιαίτερα ευαίσθητων δεδομένων. Θα πρέπει να μεταφέρονται σε χωριστό κανάλι επικοινωνίας τα κρυπτογραφημένα δεδομένα και σε χωριστό κανάλι τα κλειδιά κρυπτογράφησης. Τα κλειδιά κρυπτογράφησης θα πρέπει να αλλάζουν τουλάχιστον κάθε τρεις μήνες. Εάν χρησιμοποιούν γεννήτορες κλειδιών τότε θα πρέπει να λαμβάνεται υπόψη και η τιμή μίας τυχαίας μεταβλητής. Σε περίπτωση που τα κλειδιά κρυπτογράφησης δημιουργούνται από τους χρήστες θα πρέπει να είναι μήκους τουλάχιστον οχτώ χαρακτήρων. Τα κλειδιά κρυπτογράφησης των δεδομένων θα πρέπει να μεταφέρονται κρυπτογραφημένα στο δίκτυο. Ο αλγόριθμος κρυπτογράφησης των κλειδιών θα πρέπει να παρέχει μεγαλύτερη ασφάλεια συγκριτικά με τον αλγόριθμο κρυπτογράφησης των δεδομένων. Η χρήση κρυπτογραφικών τεχνικών σε περιβάλλον δικτύων δεδομένων απαιτεί την εξέταση και άλλων παραγόντων. Για παράδειγμα, θα πρέπει να επιβεβαιωθεί ότι τα πρωτόκολλα και ο εξοπλισμός επικοινωνίας είναι διαφανή, και επιτρέπουν την μετάδοση των διαφόρων μορφών κρυπτογραφημένης πληροφορίας χωρίς προβλήματα. Επίσης, θα πρέπει η κρυπτογραφημένη πληροφορία να μορφοποιηθεί πριν τη μετάδοση της με τρόπο

που να μην δημιουργεί προβλήματα (π.χ. να ερμηνεύεται σαν ακολουθία από χαρακτήρες ελέγχου) στις δικτυακές ή άλλες εφαρμογές που εμπλέκονται στη μετάδοση. Οι εργαζόμενοι δεν θα πρέπει να διαγράφουν από το σύστημα τη αναγνώσιμη μορφή της κρυπτογραφημένης πληροφορίας διότι εάν η αποκρυπτογράφηση αποτύχει τότε θα επέλθει οριστική απώλεια των πληροφοριών. Εάν πρόκειται να αποθηκευτεί μεγάλος όγκος ευαίσθητης πληροφορίας στο δίκτυο τότε θα πρέπει πρώτα να συμπιέζεται η πληροφορία και έπειτα να κρυπτογραφείται.

ΕΡΓΟ 30

❖ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΑΔΙΚΤΥΟΥ

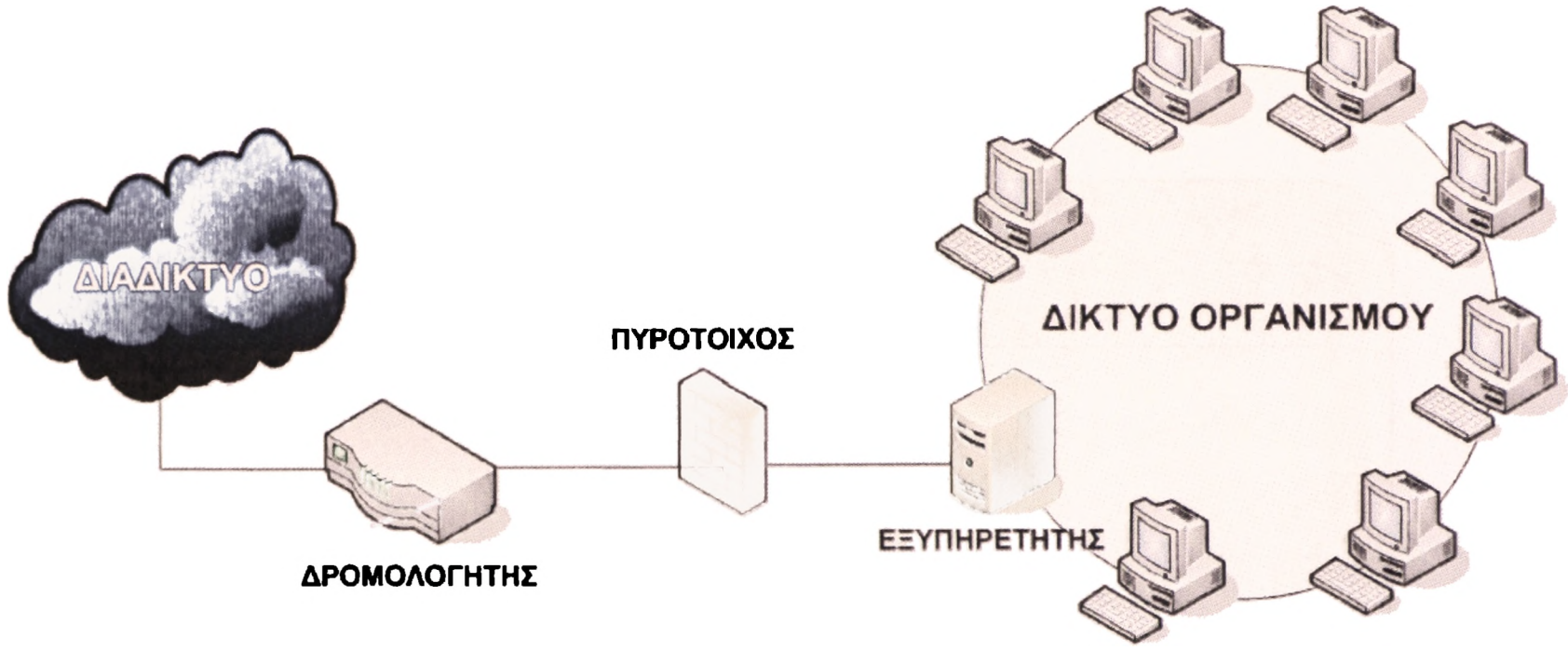
ΚΕΦΑΛΑΙΟ 6

6.1 ΑΠΑΙΤΗΣΕΙΣ ΕΠΙΧΕΙΡΗΣΗΣ

6.2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

6.1 ΑΠΑΙΤΗΣΕΙΣ ΕΠΙΧΕΙΡΗΣΗΣ

Οι επιχειρήσεις χρησιμοποιούν το Διαδίκτυο λόγω των ποικίλων και χρήσιμων υπηρεσιών που προσφέρει. Οι περισσότερες επιχειρήσεις χρησιμοποιούν τις υπηρεσίες του Διαδικτύου (Σχήμα 6-1) για να επικοινωνήσουν με άλλες επιχειρήσεις (πελάτες και προμηθευτές) με στόχο κατά κύριο λόγο τη μείωση του κόστους των συναλλαγών. Η ασφάλεια αποτελεί κρίσιμο θέμα διότι ενδέχεται μία μεμονωμένη εισβολή να αντισταθμίσει ή να ξεπεράσει τυχόν εξοικονομήσεις που έχουν γίνει από τη χρήση του Διαδικτύου και να οδηγήσει σε μεγάλες οικονομικές απώλειες για την επιχείρηση.



Σχήμα 6-1: Τυπική αρχιτεκτονική του διαδικτύου

Ακολούθως δίδεται ένας πίνακας (πίνακας 6-Α) όπου παρουσιάζονται ορισμένες υπηρεσίες που μπορεί να προσφέρει το Διαδίκτυο και το επίπεδο ασφάλειας που απαιτείται για κάθε μια από τις υπηρεσίες αυτές [site6]

	Ταυτοποίηση & Πιστοποίηση	Έλεγχος πρόσβασης	Firewall	Έλεγχος εισαγωγής λογισμικού	Κρυπτογράφηση	Χειρισμός Γεγονότων
Απομακρυσμένη πρόσβαση	X	X	X		X	
Ηλεκτρονικό ταχυδρομείο	X			X	X	
Έρευνα		X	X	X		
Ηλεκτρονικό εμπόριο	X	X	X	X	X	X

Πίνακας 6-Α: Υπηρεσίες Διαδικτύου και απαιτήσεις ασφάλειας

6.1.1 ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ (REMOTE ACCESS)

Σε πολλές περιπτώσεις είναι απαραίτητη η απομακρυσμένη πρόσβαση κάποιου χρήστη στο εταιρικό δίκτυο. Μερικές φορές είναι αναγκαίο η δυνατότητα αυτή να δίνεται ακόμη και σε εξωτερικούς συνεργάτες, προμηθευτές ή και πελάτες. Οι απομακρυσμένες συνδέσεις επιτυγχάνονται με διάφορους τρόπους, όπως με dial-in modems, DSL, Εικονικά Ιδιωτικά Δίκτυα (VPNs) κ.λπ. Η πολιτική ασφάλειας που ορίζει το γενικό πλαίσιο χρήσης της απομακρυσμένης πρόσβασης συνοψίζεται στα παρακάτω:

- Οι χρήστες είναι υποχρεωμένοι να μην παρακάμπτουν τα δικαιώματα πρόσβασης που έχουν με τη σύνδεση αυτή.
- Δεν θα πρέπει να κάνουν χρήση της σύνδεσης αυτής για προσωπικούς λόγους, π.χ. Διαδίκτυο, παρά μόνο για σκοπούς που έχουν άμεση σχέση με την εργασία τους.
- Όταν μεταφέρουν αρχεία μέσω αυτής της σύνδεσης οφείλουν να τηρούν την πολιτική ασφάλειας που ισχύει για τις διαβαθμισμένες πληροφορίες (κρυπτογράφηση, ταυτοποίηση). Επίσης θα πρέπει να τηρούν τις αντίστοιχες πολιτικές χρήσης Διαδικτύου και ηλεκτρονικού ταχυδρομείου.
- Είναι απαραίτητο να υπάρχουν οι κατάλληλοι μηχανισμοί που να ελέγχουν την απομακρυσμένη σύνδεση και να διαχειρίζονται από το Τμήμα Ασφάλειας της εταιρίας.
- Ο έλεγχος πρόσβασης θα πρέπει να γίνεται με προηγμένους μηχανισμούς ταυτοποίησης, π.χ. κωδικοί μιας χρήσης, PKI/δημόσια και ιδιωτικά κλειδιά.
- Οι υπολογιστές που είναι συνδεδεμένοι με το εταιρικό δίκτυο δεν θα είναι συνδεδεμένοι και με άλλο δίκτυο ταυτόχρονα.
- Ο εξοπλισμός που χρησιμοποιείται για τις απομακρυσμένες συνδέσεις θα πρέπει να εγκρίνεται από το Τμήμα Ασφάλειας και να προβλέπει μηχανισμούς ταυτοποίησης/αναγνώρισης.
- Όλοι οι υπολογιστές που χρησιμοποιούνται θα πρέπει να διαθέτουν ενημερωμένο λογισμικό καταπολέμησης ιών (anti-virus).

6.1.2 DIAL-IN

Για την πρόσβαση από μακριά συνήθως χρησιμοποιούνται μισθωμένες τηλεφωνικές γραμμές. Για την ασφάλεια του δικτύου θα πρέπει να ελέγχονται και οι γραμμές των modems. Παρόλο που οι διαποδιαμορφωτές είναι ένας εύκολος τρόπος πρόσβασης σε ένα ιστότοπο, μπορούν να προκαλέσουν αρκετά προβλήματα στην ασφάλεια. Οι γραμμές modem θα πρέπει να εγκαθίστανται μετά από κατάλληλη εξουσιοδότηση. Για τις γραμμές αυτές θα πρέπει να τηρείται αρχείο το οποίο θα ενημερώνεται τακτικά για όλες τις ενέργειες που έχουν προηγηθεί.

6.1.2.1 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΤΗΛΕΦΩΝΙΚΩΝ ΓΡΑΜΜΩΝ ΤΩΝ MODEMS

Πιστοποίηση των Dial-In χρηστών

Οι dial-in χρήστες θα πρέπει να πιστοποιούνται πριν από την προσπέλαση οποιασδήποτε συσκευής του συστήματος. Σε κάθε περίπτωση μια τηλεφωνική γραμμή μπορεί να μπλοκαριστεί και ο εισβολέας να δει την πληροφορία που περνάει από την γραμμή. Ενδείκνυται η one-time αλλαγή του κωδικού. Πολλές φορές οι χρήστες δίνουν λάθος τον κωδικό τους. Στην περίπτωση αυτή θα πρέπει να δίνεται στο χρήστη δυνατότητα επανάληψης της διαδικασίας μέχρι τρεις φορές. Αν τελικά ο χρήστης δεν συνδεθεί είναι καλό να μην αναφέρεται σε ποιο σημείο (login ή password) έγινε το λάθος.

Χρήση Callback

Μια άλλη δυνατότητα που μπορεί να δώσει ο διαχειριστής στον dial-in εξυπηρετητή είναι αυτή του call-back (ο χρήστης καλεί και αφού πιστοποιηθεί η αυθεντικότητα του, το σύστημα τον αποσυνδέει και καλεί το χρήστη σε συγκεκριμένο αριθμό). Με το call-back μπορεί να ελεγχθεί κάποιος εισβολέας αφού κατά το call-back υπάρχει το νούμερο του δικαιούχου χρήστη μόνο.

Καταγραφή όλων των login

Θα πρέπει όλο το σύμπλεγμα των dial-in συσκευών και συνδέσεων να καταγράφεται τόσο για τα dial-in όσο και τα dial-out τηλεφωνήματα που γίνονται. Αυτό γίνεται με καταγραφικό σύστημα στο τηλεφωνικό κέντρο.

Επιλογή τον κατάλληλου μηνύματος στην σύνδεση

Θα πρέπει να ελέγχεται η πληροφορία που εμφανίζεται στα banner. Θα πρέπει να είναι σύντομη χωρίς να δίνει στοιχεία σχετικά με τον τύπο του υλικού του host ή το λειτουργικό σύστημα που είναι εγκατεστημένο στο host. Θα μπορούσε να χρησιμοποιηθεί και ένας «τυφλός κωδικός» (blind password) (π.χ. να μην δίνεται καμία απάντηση σε μια εισερχόμενη κλήση μέχρι ο χρήστης πληκτρολογήσει κάποιο κωδικό). Η διαδικασία αυτή εξομοιώνει ένα «νεκρό διαποδιαμορφωτή» (dead modem).

Πιστοποίηση Dial-Out

Σημαντικό ζητήματα είναι η πιστοποίηση της αυθεντικότητας των dial-out χρηστών κύρια για λόγους ασφάλειας αλλά και γιατί ο οργανισμός πληρώνει τις κλήσεις. Ποτέ δεν πρέπει να επιτρέπεται dial-out δυνατότητα από ένα σημείο που δεν ελέγχεται η δυνατότητα για dial-in. Είναι πολύ δύσκολο να ανιχνευτούν οι κινήσεις ενός hacker που περνά από πολλά διαφορετικά σημεία στον οργανισμό. Τουλάχιστον δεν πρέπει να επιτρέπεται το ίδιο modem να λειτουργεί με δυνατότητα dial-in και dial-out.

6.1.3 MOBILE COMPUTING

Η χρήση των φορητών υπολογιστών έχει αυξηθεί δραματικά τα τελευταία χρόνια εξαιτίας της συνεχόμενης μείωσης του κόστους, του μεγέθους και του βάρους των φορητών υπολογιστών. Η χρήση φορητών υπολογιστών περιλαμβάνει τη χρήση των φορητών υπολογιστών τόσο για τις λειτουργίες της επιχείρησης όσο και για τη σύνδεση με το δίκτυο της επιχείρησης. Για να επιτευχθεί η σύνδεση χρησιμοποιείται telnet ή dial-in ενώ παρουσιάζονται επιπρόσθετες ευπάθειες όπως:

- Η θέση του φορητού υπολογιστή (laptop) αλλάζει συχνά έτσι τα dial-back modems δεν μπορούν να χρησιμοποιηθούν για να ελεγχθεί η πρόσβαση.
- Ο φορητός υπολογιστής συνήθως χρησιμοποιείται σε δημόσιους χώρους και έτσι τα δεδομένα και οι κωδικοί εκτίθενται σε κίνδυνο.
- Ο φορητός υπολογιστής τοποθετείται σε μη ασφαλή περιβάλλοντα όπως είναι τα ξενοδοχεία και έτσι υπάρχει κίνδυνος κλοπής των στοιχείων που έχουν αποθηκευτεί.

6.1.4 ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΣΥΝΔΕΣΗ (TELNET)

Το telnet και οι εντολές remote login του UNIX χρησιμοποιούνται για τη σύνδεση με άλλους υπολογιστές βάσει των συνδέσεων δικτύου. Οι προσωπικοί υπολογιστές που διαθέτουν το TCP/IP λογισμικό παρέχουν αυτή τη δυνατότητα. Η υπηρεσία telnet απαιτεί τη μεταφορά του username και του password μέσω του δικτύου σε καθαρή μορφή το οποίο αποτελεί προφανής ευπάθεια.

6.1.5 ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

Το ηλεκτρονικό ταχυδρομείο αποτελεί μία σημαντική υπηρεσία για την επικοινωνία των επιχειρήσεων με πελάτες, προμηθευτές και συνεργάτες και είναι η κύρια αιτία που ώθησε την ανάπτυξη του Διαδικτύου. Εν τούτοις η υπηρεσία αυτή παρουσιάζει ευπάθειες όπως:

- Οι διευθύνσεις του ηλεκτρονικού ταχυδρομείου εύκολα ξεγελιούνται και είναι σχεδόν αδύνατο να πιστοποιηθεί ο αποστολέας του μηνύματος εξετάζοντας μόνο την ηλεκτρονική του διεύθυνση.
- Τα μηνύματα που αποστέλλονται μπορούν εύκολα να τροποποιηθούν. Για παράδειγμα το standard SMTP mail δεν παρέχει έλεγχο ακεραιότητας
- Τα περιεχόμενα του μηνύματος μπορούν να διαβαστούν από κάθε ενδιάμεσο σταθμό.
- Δεν υπάρχει εγγύηση παράδοσης. Ορισμένα συστήματα ταχυδρομείου υποστηρίζουν την αποστολή απόκρισης όταν ο εξυπηρετητής του χρήστη λάβει το μήνυμα.

6.1.6 ΕΡΕΥΝΑ

Για να πραγματοποιηθεί η αναζήτηση στο Διαδίκτυο απαιτείται λογισμικό πελάτη (client software). Τύποι λογισμικού πελάτη είναι οι ακόλουθοι :

File Transfer Protocol: Το FTP λογισμικό χρησιμοποιείται για την σύνδεση με μακρινά συστήματα και για την μεταφορά αρχείων.

World Wide Web: Τα προγράμματα πλοήγησης (web browsers) έχουν κατακλύσει την αγορά και χρησιμοποιούνται για την ανάκτηση των πληροφοριών από το Διαδίκτυο. Το λογισμικό των προγραμμάτων πλοήγησης καταγράφει ευαίσθητες πληροφορίες όπως τον

τύπο του προγράμματος πλοήγησης που χρησιμοποιήθηκε, τον τελευταίο ιστότοπο της επίσκεψης, την διεύθυνση του ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται στο πρόγραμμα πλοήγησης κ.λ.π.

6.1.7 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. Το ηλεκτρονικό εμπόριο αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως. Το ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών. Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και φαξ. Το ηλεκτρονικό εμπόριο διακρίνεται σε έμμεσο και άμεσο. Ο πρώτος όρος χρησιμοποιείται όταν πρόκειται για την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο.

Άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών. Για την πραγματοποίηση του ηλεκτρονικού εμπορίου χρησιμοποιούνται ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονική ανταλλαγή δεδομένων (EDI), συναλλαγές πληροφορίας και οικονομικές συναλλαγές. Κάθε μία από τις δραστηριότητες αυτές απαιτεί διαφορετικό επίπεδο ασφάλειας.

6.2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στις περισσότερες εταιρίες η χρήση του Διαδικτύου αποτελεί ένα από τα κυριότερα εργαλεία για τη διεκπεραίωση καθημερινών, βασικών λειτουργιών. Οι κίνδυνοι όμως είναι αρκετοί. Για παράδειγμα, οι πληροφορίες που αποστέλλονται μέσω του Διαδικτύου χωρίς τη λήψη ειδικών μέτρων μπορούν να διαβαστούν ή και να αλλαχθούν. Το εσωτερικό δίκτυο μιας εταιρίας μπορεί να γίνει στόχος κακόβουλων ενεργειών και να καταστεί αδύνατη η πρόσβαση από τους εξουσιοδοτημένους χρήστες, με αποτέλεσμα να καταργούνται οι όροι που αναφέρθηκαν παραπάνω, όπως «εμπιστευτικότητα», «ακεραιότητα» και «διαθεσιμότητα». Οι χρήστες θα πρέπει να πειστούν ότι η χρήση του Διαδικτύου επηρεάζει άμεσα τη φήμη και την αξιοπιστία της επιχείρησης εφόσον καταγράφεται κάθε επίσκεψη σε οποιοδήποτε ιστότοπο του Διαδικτύου.

6.2.1 ΠΟΛΙΤΙΚΗ ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Η πολιτική ασφάλειας που θα αναπτυχθεί στοχεύει να δώσει τις κατευθυντήριες γραμμές για την ασφαλή χρήση του Διαδικτύου (Internet). Στόχος είναι να προσδιοριστούν οι

διαδικασίες και οι έλεγχοι έτσι ώστε το Διαδίκτυο να χρησιμοποιηθεί ως ασφαλές μέσο κάλυψης των αναγκών της επιχείρησης. Ακολούθως παρατίθενται ορισμένες σημαντικές πολιτικές αποδεκτής χρήσης του Διαδικτύου, ανάλογα με το επίπεδο επικινδυνότητας που χαρακτηρίζει την επιχείρηση [Site6a].

ΧΑΜΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Το Διαδίκτυο θεωρείται ως ένα πολύτιμο προτέρημα μιας επιχείρησης. Οι χρήστες ενθαρρύνονται να χρησιμοποιήσουν το Διαδίκτυο και να ερευνήσουν τις χρήσεις του. Με μια τέτοια ανοικτή πρόσβαση, οι υπάλληλοι πρέπει να διατηρήσουν ένα επιμελές και επαγγελματικό εργασιακό περιβάλλον. Οι υπάλληλοι δεν μπορούν να χρησιμοποιήσουν το Διαδίκτυο για προσωπικούς εμπορικούς λόγους, δεν μπορούν να έχουν πρόσβαση σε οποιεσδήποτε άσεμνες ή πορνογραφικές σελίδες, και δεν μπορούν να έχουν πρόσβαση ή να χρησιμοποιήσουν πληροφορίες που θα εξετάζονταν και θα θεωρούνταν ως παρενόχληση. Η πρόσβαση στο Διαδίκτυο από έναν κάτοχο υπολογιστή της επιχείρησης ή μέσω των κατόχων συνδέσεων της επιχείρησης πρέπει να εμμείνει σε όλες τις ίδιες πολιτικές που ισχύουν όταν κάνουν χρήση μέσα από τις εγκαταστάσεις της επιχείρησης. Οι υπάλληλοι δεν πρέπει να επιτρέψουν στα οικογενειακά μέλη ή άλλους μη-υπαλλήλους να έχουν πρόσβαση στα συστήματα ηλεκτρονικών υπολογιστών της επιχείρησης. Οι υπάλληλοι που κάνουν κακή χρήση τέτοιων προνομίων υπόκεινται στον έλεγχο της δραστηριότητας των συστημάτων ηλεκτρονικών υπολογιστών και της πειθαρχικής δράσης τους, που κυμαίνεται από λεκτικές επιπλήξεις μέχρι την απόλυση ή τη νομική συνέχιση. Είναι αδύνατο να καθοριστεί όλη η πιθανή αναρμόδια χρήση, επομένως η πειθαρχική δράση μπορεί να εμφανιστεί μετά από άλλες ενέργειες εάν οι περιστάσεις την επιτρέπουν. Τα παραδείγματα συμπεριφορών που κρίνονται απαράδεκτες και που οδηγούν στην πειθαρχική δράση περιλαμβάνουν:

- Αναρμόδιες προσπάθειες για είσοδο σε οποιοδήποτε υπολογιστή.
- Χρησιμοποίηση του χρόνου και των πόρων επιχείρησης για προσωπικό κέρδος.
- Κλοπή ηλεκτρονικών αρχείων ή αντιγραφή χωρίς άδεια.
- Αποστολή ή ταχυδρόμηση εμπιστευτικών αρχείων της επιχείρησης έξω από την επιχείρηση ή μέσα στην επιχείρηση σε αναρμόδιο προσωπικό.
- Άρνηση συνεργασίας με μια λογική έρευνα ασφάλειας.
- Αποστολή επιστολών αλυσίδων μέσω του ηλεκτρονικού ταχυδρομείου.

ΜΕΣΑΙΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Τα συστήματα ηλεκτρονικών υπολογιστών μιας επιχείρησης και τα δίκτυα παρέχονται για την επιχειρησιακή χρήση μόνο. Η περιστασιακή, λογική προσωπική χρήση επιτρέπεται. Οποιαδήποτε χρήση που γίνεται αντιληπτή ως παράνομη, ως παρενόχληση, ως επίθεση, ως παραβίαση άλλων πολιτικών της επιχείρησης ή οποιαδήποτε χρήση που θα δρούσε ενάντια στην επιχείρηση μπορούν να είναι η βάση για την πειθαρχική δράση συμπεριλαμβανομένης μέχρι και της λήξης ή της δικαστικής δράσης. Μια άλλη προσέγγιση στη δήλωση των ανωτέρω μπορεί να είναι η εξής:

Τα συστήματα και ο εξοπλισμός επικοινωνιών της επιχείρησης, συμπεριλαμβανομένων των συστημάτων ηλεκτρονικού ταχυδρομείου και Διαδικτύου, μαζί με το σχετικό υλικό και το λογισμικό τους είναι για επίσημους και εξουσιοδοτημένους λόγους μόνο. Οι διευθυντές μπορούν να εγκρίνουν την τυχαία χρήση που: δεν παρεμποδίζει την απόδοση ή τα επαγγελματικά καθήκοντα, που είναι λογικής διάρκειας και συχνότητας, που εξυπηρετεί ένα νόμιμο ενδιαφέρον της επιχείρησης όπως η ενίσχυση των επαγγελματικών ενδιαφερόντων ή

της εκπαίδευσης και που δεν επιβαρύνει το σύστημα ή δεν δημιουργεί οποιαδήποτε πρόσθετη δαπάνη στην επιχείρηση.

Οι διευθυντές είναι αρμόδιοι να εξασφαλίσουν ότι το διορισμένο προσωπικό καταλαβαίνει την αποδεκτή πολιτική χρήσης Διαδικτύου. Η πρόσβαση στο Διαδίκτυο θα πρέπει να γίνεται μόνο μέσα από συγκεκριμένες εξόδους (gateways) που τηρούν τους μηχανισμούς έλεγχου και την πολιτική ασφάλειας της εταιρίας. Οι υπάλληλοι δεν πρέπει να επιτρέπουν σε οικογενειακά μέλη ή άλλους μη-υπαλλήλους να έχουν πρόσβαση στα συστήματα ηλεκτρονικών υπολογιστών της επιχείρησης. Κάθε υπολογιστικό σύστημα της επιχείρησης θα πρέπει να προστατεύεται με συνθηματικό προκειμένου να εμποδιστεί η αποκάλυψη ευαίσθητης πληροφορίας ή μηνυμάτων σε τρίτους.

ΥΨΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Οι χρήστες θα πρέπει να χρησιμοποιούν το Διαδίκτυο μόνο για σκοπούς που εξυπηρετούν και έχουν άμεση σχέση με την εργασία τους. Ένας χωριστός δημόσιος κεντρικός υπολογιστής πρόσβασης στο Διαδίκτυο παρέχεται για την προσωπική χρήση του υπαλλήλου. Αυτή η υπηρεσία πρέπει να χρησιμοποιείται με την επαγγελματική διακριτικότητα. Μόνο εκείνες οι περιοχές στις οποίες η επιχείρηση έχει εγκρίνει την πρόσβαση είναι διαθέσιμες μέσω αυτής της υπηρεσίας. Οι εξυπηρετητές (servers) που περιέχουν διαβαθμισμένες πληροφορίες δεν πρέπει να είναι προσβάσιμοι από το Διαδίκτυο με απλό λογισμικό πλοήγησης. Οποιαδήποτε χρήση γίνεται αντιληπτή ως παράνομη, ως παρενόχληση και δυσαρέσκεια ή ως παραβίαση άλλων πολιτικών της επιχείρησης μπορεί να είναι η βάση για την πειθαρχική δράση συμπεριλαμβανομένης μέχρι και της απόλυσης ή της δικαστικής δράσης. Η διαχείριση της επιχείρησης διατηρεί το δικαίωμα να ελέγχει περιοδικά την χρήση των υπαλλήλων οποιονδήποτε συστημάτων ηλεκτρονικών υπολογιστών ή δικτύου. Η πρόσβαση στο Διαδίκτυο από έναν προσωπικό υπολογιστή πρέπει να εμμείνει σε όλες τις ίδιες πολιτικές που ισχύουν όταν χρησιμοποιείται από μέσα από τις εγκαταστάσεις της επιχείρησης. Οι υπάλληλοι δεν πρέπει να επιτρέπουν σε οικογενειακά μέλη ή άλλους μη-υπαλλήλους να έχουν πρόσβαση στα συστήματα ηλεκτρονικών υπολογιστών της επιχείρησης.

6.2.2 ΕΛΕΓΧΟΣ ΕΙΣΑΓΩΓΗΣ ΛΟΓΙΣΜΙΚΟΥ

Τα δεδομένα στους υπολογιστές αλλάζουν σε μόνιμη βάση εφόσον περιοδικά εγκαθίστανται νέες εφαρμογές, καθημερινά παραλαμβάνονται ηλεκτρονικά μηνύματα και αντλούνται πληροφορίες από το Διαδίκτυο. Οποιαδήποτε αλλαγή στα δεδομένα εμπεριέχει τον κίνδυνο εισαγωγής ιομορφικού λογισμικού, καταστροφής της διαμόρφωσης του συστήματος ή προσβολής των συμβάσεων άδειας λογισμικού. Ο έλεγχος εισαγωγής λογισμικού απαιτείται να αντιμετωπίσει τις ακόλουθες προκλήσεις :

- Πρόληψη, Ανίχνευση και Διαγραφή Ιών, «Σκουληκιών» (Worms) και Δούρειων Ίππων.
- Παραβιάσεις στις άδειες λογισμικού.

Οι επιχειρήσεις που επιτρέπουν την εγκατάσταση λογισμικού από το Διαδίκτυο θα πρέπει να χρησιμοποιούν υποχρεωτικά λογισμικό ανίχνευσης ιών στο χρησιμοποιούμενο

πυρότοιχο (firewall). Τα εργαλεία ανίχνευσης ιών περιορίζονται στον εντοπισμό κυρίως γνωστών ιομορφών.

Απαιτείται να υπάρχουν οδηγίες για την πρόληψη, ανίχνευση και διαγραφή των ιομορφών. Η συχνότητα εγκατάστασης νέου λογισμικού αυξάνει την πιθανότητα εισαγωγής ιομορφικού λογισμικού. Προφανώς στην εκτίμηση του κόστους εισβολής του ιομορφικού λογισμικού θα πρέπει να συνυπολογίζονται και οι τυχόν μολύνσεις που έχουν μεταδοθεί στα υπολογιστικά περιβάλλοντα πελατών και προμηθευτών. Προφανώς το κόστος δεν είναι μόνο οικονομικό εφόσον η γνωστοποίηση της εισβολής ιομορφικού λογισμικού επηρεάζει αρνητικά την αξιοπιστία και το κύρος της επιχείρησης.

6.2.2.1 ΠΟΛΙΤΙΚΕΣ ΠΡΟΛΗΨΗΣ, ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΔΙΑΓΡΑΦΗΣ ΙΟΜΟΡΦΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

Η πολιτική ασφάλειας για το ιομορφικό λογισμικό θα πρέπει να στοχεύει κυρίως στην πρόληψη. Ακολουθεί διάκριση της πολιτικής ασφάλειας ιομορφικού λογισμικού ανάλογα με το επίπεδο επικινδυνότητας που χαρακτηρίζει την επιχείρηση/οργανισμό [Site6a].

ΧΑΜΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Οι πολιτικές ελέγχου εισαγωγής λογισμικού Θα πρέπει επικεντρώνονται στην εκπαίδευση των χρηστών για τον έλεγχο (scanning) του συστήματος τους.

ΠΡΟΛΗΨΗ:

Οι χρήστες θα πρέπει να πειστούν ότι υπάρχει σοβαρός κίνδυνος εισαγωγής ιομορφικού λογισμικού από το διαδίκτυο. Οι χρήστες θα πρέπει να εκπαιδευτούν στη χρήση εργαλείων ανίχνευσης ιών.

ΑΝΙΧΝΕΥΣΗ:

Θα πρέπει να χρησιμοποιούνται σε εβδομαδιαία βάση εργαλεία ανίχνευσης ιων.

Οι εργαζόμενοι θα πρέπει να αναφέρουν στο διαχειριστή του συστήματος τα αποτελέσματα της ανίχνευσης.

Οι εργαζόμενοι θα πρέπει να ενημερώνουν τον διαχειριστή του συστήματος για τυχόν μη αναμενόμενη συμπεριφορά του συστήματος ή κάποιας εφαρμογής που χρησιμοποιούν.

Όταν ενημερωθεί ο διαχειριστής του συστήματος για την εισβολή κάποιου ιού θα πρέπει να ενημερώνει όλους τους χρήστες που έχουν πρόσβαση στο «μολυσμένο σύστημα» ότι υπάρχει πιθανότητα μετάδοσης του ιού.

ΔΙΑΓΡΑΦΗ:

Οποιοσδήποτε υπολογιστής είναι μολυσμένος θα πρέπει άμεσα να αποσυνδέεται από το δίκτυο.

Ο υπολογιστής δεν θα πρέπει να επανασυνδέεται στο δίκτυο έως ότου ο διαχειριστής του συστήματος πιστοποιήσει ότι η διαγραφή του ιού έχει ολοκληρωθεί με επιτυχία.

Για τη διαγραφή του ιού θα πρέπει να χρησιμοποιηθεί εργαλείο ανίχνευσης ιών. Εάν το εργαλείο αυτό δεν καταφέρει να διαγράψει τον ιό θα πρέπει να διαγραφεί όλο το λογισμικό του συστήματος συμπεριλαμβανομένων και των αρχείων εκκίνησης

ΜΕΣΑΙΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

ΠΡΟΛΗΨΗ:

Οι χρήστες θα πρέπει να πειστούν ότι υπάρχει σοβαρός κίνδυνος εισαγωγής ιομορφικού λογισμικού από το Διαδίκτυο.

Μόνο οι διαχειριστές του συστήματος θα πρέπει να αντλούν λογισμικό από το Διαδίκτυο. Η εγκατάσταση του λογισμικού θα πρέπει να γίνεται μόνο εφόσον ο διαχειριστής του συστήματος έχει ελέγξει την ποιότητα του.

Το λογισμικό ανίχνευσης ιών θα πρέπει να εγκατασταθεί στους εξυπηρετητές αρχείων (file servers) προκειμένου να περιοριστεί η μετάδοση του ιού στο δίκτυο.

Οι εξυπηρετητές αρχείων θα πρέπει να ελέγχονται για ιομορφικό λογισμικό σε ημερήσια βάση.

Στους σταθμούς εργασίας θα πρέπει να χρησιμοποιείται λογισμικό ανίχνευσης ιών όταν εισάγονται νέα στοιχεία από το Διαδίκτυο.

Τα εισερχόμενα ηλεκτρονικά μηνύματα θα πρέπει να ελέγχονται για ιομορφικό λογισμικό.

Το λογισμικό ανίχνευσης ιομορφών θα πρέπει να αναβαθμίζεται σε μηνιαία βάση.

ΑΝΙΧΝΕΥΣΗ:

Τα εργαλεία ανίχνευσης ιομορφικού λογισμικού θα πρέπει να χρησιμοποιούνται σε όλα τα υπολογιστικά συστήματα σε ημερήσια βάση.

Οι εργαζόμενοι θα πρέπει να ενημερώνουν τον διαχειριστή του συστήματος για τυχόν μη αναμενόμενη συμπεριφορά του συστήματος ή κάποιας εφαρμογής που χρησιμοποιούν.

Όλα τα δεδομένα που εισάγονται στους υπολογιστές (e-mail, ftp) θα πρέπει να εξετάζονται για ιούς προτού χρησιμοποιηθούν.

Το αρχείο καταγραφής των αποτελεσμάτων ανίχνευσης θα πρέπει να ελέγχεται από το διαχειριστή του συστήματος.

Όταν ενημερωθεί ο διαχειριστής του συστήματος για την εισβολή κάποιου ιού θα πρέπει να ενημερώνει όλους τους χρήστες που έχουν πρόσβαση στο «μολυσμένο σύστημα» ότι υπάρχει πιθανότητα μετάδοσης του ιού.

ΔΙΑΓΡΑΦΗ:

Όμοια με την πολιτική διαγραφής για τις επιχειρήσεις χαμηλού επιπέδου επικινδυνότητας.

ΥΨΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Στα συστήματα υψηλού κινδύνου υπάρχουν δεδομένα και εφαρμογές ιδιαίτερα ευαίσθητες για την επιχείρηση και οποιαδήποτε προσβολή από ιομορφικό λογισμικό θα προκαλέσει απώλειες σε πολύτιμο χρόνο, δεδομένα, και ενδεχόμενα θα επηρεάσει αρνητικά τη φήμη και την αξιοπιστία της επιχείρησης.

ΠΡΟΛΗΨΗ:

Ο διαχειριστής του συστήματος θα πρέπει να εγκρίνει την εγκατάσταση μίας νέας εφαρμογής.

Απαγορεύεται η άντληση λογισμικού από το Διαδίκτυο.

Το λογισμικό ανίχνευσης ιών θα πρέπει να εγκατασταθεί στους εξυπηρετητές αρχείων προκειμένου να περιοριστεί η μετάδοση του ιού στο δίκτυο.

Στους σταθμούς εργασίας θα πρέπει να χρησιμοποιείται λογισμικό ανίχνευσης ιών όταν εισάγονται νέα στοιχεία από το Διαδίκτυο.

Τα εισερχόμενα ηλεκτρονικά μηνύματα θα πρέπει να ελέγχονται για ιομορφικό λογισμικό

Η ανίχνευση ιομορφικού λογισμικού θα πρέπει να γίνεται στο διαθέσιμο «Τείχος Ασφάλειας» (firewall) όπου γίνεται και ο έλεγχος πρόσβασης στο δίκτυο.

Το λογισμικό ανίχνευσης ιομορφών θα πρέπει να αναβαθμίζεται σε μηνιαία βάση.

ΑΝΙΧΝΕΥΣΗ:

Όμοια με την πολιτική ανίχνευσης για συστήματα χαμηλού κινδύνου.

Επιπλέον, το λογισμικό πρώτα θα πρέπει να εγκαθίσταται δοκιμαστικά σε κάποιο υπολογιστικό σύστημα και μόνο εάν εγκριθεί από τον διαχειριστή του συστήματος θα τίθεται σε εφαρμογή.

ΔΙΑΓΡΑΦΗ:

Όμοια με την πολιτική διαγραφής για τις επιχειρήσεις χαμηλού επιπέδου επικινδυνότητας.

6.2.2.2 ΕΛΕΓΧΟΣ ΠΑΡΑΒΙΑΣΕΩΝ ΣΕ ΑΔΕΙΕΣ ΛΟΓΙΣΜΙΚΟΥ

Το Διαδίκτυο χρησιμοποιείται από πολλές εταιρείες ως μέσο διανομής του λογισμικού. Πολλές φορές οι εταιρείες μέσω του Διαδικτύου προσφέρουν δοκιμαστικές εφαρμογές οι οποίες έχουν περιορισμένες δυνατότητες και ορισμένη περίοδο χρήσης. Από ορισμένες επιχειρήσεις δίδεται η δυνατότητα δοκιμαστικής χρήσης του λογισμικού. Σε περίπτωση εμπορικής χρήσης του λογισμικού αυτού απαιτείται η επιχείρηση να είναι νόμιμος κάτοχος του προϊόντος. Αν αγνοηθούν οι περιορισμοί αυτοί η επιχείρηση εκτίθεται σε κίνδυνο διότι έχει παραβιάσει την συμφωνία με τον προμηθευτή του λογισμικού. Η πολιτική ασφάλειας θα πρέπει να προσδιορίζει τον τρόπο άντλησης εμπορικών εφαρμογών από το Διαδίκτυο έτσι ώστε να μην παραβιάζονται οι άδειες του λογισμικού. Συγκεκριμένα:

ΧΑΜΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Οι δοκιμαστικές εκδόσεις του λογισμικού που αντλείται από το Διαδίκτυο θα πρέπει να διαγράφονται από το σύστημα όταν εκπνεύσει η περίοδος δοκιμής ή θα πρέπει η επιχείρηση να ακολουθήσει τη σχετική διαδικασία προκειμένου να γίνει νόμιμος κάτοχος του προϊόντος.

ΜΕΣΑΙΟ-ΥΨΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Εμπορικό λογισμικό δεν θα πρέπει να αντλείται από το Διαδίκτυο χωρίς την έγκριση του διαχειριστή του συστήματος. Το λογισμικό που χρησιμοποιεί η επιχείρηση θα πρέπει να εγκαθίσταται μόνο από το διαχειριστή του συστήματος. Ο διαχειριστής του συστήματος θα πρέπει να ελέγχει περιοδικά εάν η επιχείρηση είναι νόμιμος κάτοχος του λογισμικού που χρησιμοποιεί. Σε περίπτωση που κάποιος υπάλληλος παραβιάσει την πολιτική αυτή θα πρέπει να υφίσταται τις σχετικές συνέπειες.

6.2.3 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΣΦΑΛΕΙΑΣ

Στα πλαίσια της πολιτικής διαχείρισης θα πρέπει να οριστούν οι υπεύθυνοι ασφαλείας,

οι ποινές που θα επιβληθούν σε περίπτωση παραβίασης της πολιτικής ασφαλείας, τα πλαίσια χρήσης του Διαδικτύου καθώς και τι θεωρεί η επιχείρηση ως «μυστικότητα» (privacy) των εργαζομένων. Η επιτυχία της πολιτικής ασφαλείας εξαρτάται άμεσα από τις ικανότητες και τα προσόντα των διαχειριστών της πολιτικής αυτής. Οι διαχειριστές του δικτύου ευθύνονται για την εφαρμογή μέτρων ασφαλείας για τη διασύνδεση του τοπικού δικτύου με το Διαδίκτυο. Εάν υπάρχουν περισσότεροι από ένας διαχειριστές δικτύου (διαχειριστής τοπικού δικτύου-LAN, διαχειριστής πυρότοιχου-firewall) είναι απαραίτητο οι ρόλοι τους να εναρμονιστούν.

Η επιχείρηση θα πρέπει να ορίσει υπεύθυνο ασφαλείας ο οποίος απαιτείται να έχει άμεση συνεργασία με το διαχειριστή του δικτύου. Ο υπεύθυνος ασφαλείας του Διαδικτύου θα πρέπει να έχει τις τεχνικές γνώσεις για την εγκατάσταση του φράγματος ασφαλείας και θα πρέπει απαραίτητα να επιθεωρεί τα audit logs. Συνήθως ως υπεύθυνος ασφαλείας επιλέγεται ο διαχειριστής δικτύου. Η επιλογή προσωπικού ασφαλείας για τις επιχειρήσεις υψηλού κινδύνου θα πρέπει πραγματοποιείται με επισταμένη προσοχή.

Αναμένονται παραβιάσεις στην πολιτική ασφαλείας του Διαδικτύου που ορίζει η επιχείρηση. Επομένως θα πρέπει να προσδιοριστούν και οι ανάλογες ποινές σε περίπτωση που παραβιάζεται η πολιτική αυτή. Οι ποινές κυμαίνονται από περιορισμό των δικαιωμάτων πρόσβασης έως επιβολή οικονομικών κυρώσεων. Σε περίπτωση που παρατηρηθεί χρήση λογισμικού όπου η εταιρεία δεν είναι νόμιμος κάτοχος, τότε θα πρέπει να επιβάλλεται οικονομική κύρωση στον υπεύθυνο. Σε περίπτωση που μη εξουσιοδοτημένος υπάλληλος αποκτήσει πρόσβαση σε ευαίσθητες ή εμπιστευτικές πληροφορίες και εκούσια τις αποκαλύψει σε τρίτους τότε θα πρέπει να απομακρύνεται από την εταιρεία.

ΚΕΦΑΛΑΙΟ 7ο

7.1 ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ (WORLD WIDE WEB)

7.2 IPSec

7.1 ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ (WORLD WIDE WEB – WWW)

Ο Παγκόσμιος Ιστός (World Wide Web – WWW) είναι ένα σύστημα ανταλλαγής πληροφοριών μέσα από το Διαδίκτυο. Σημαντικά συστατικά του στοιχεία είναι οι εξυπηρετητές Ιστού (web servers) και τα προγράμματα πλοήγησης (web browsers). Οι εξυπηρετητές Ιστού διαχειρίζονται και διανέμουν τις πληροφορίες στο Διαδίκτυο. Τα προγράμματα πλοήγησης βοηθούν τους χρήστες να αποκτήσουν πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στους εξυπηρετητές Ιστού και να τις προβάλουν στην οθόνη του χρήστη.

Πολλοί οργανισμοί χρησιμοποιούν εξυπηρετητές Ιστού, ο πηγαίος κώδικας των οποίων είναι ελεύθερα διαθέσιμος στο Διαδίκτυο. Μολονότι αυτό επιτρέπει τη δοκιμή και τον έλεγχο του προγράμματος, δίνει την δυνατότητα σε κάποιον, που έχει τις απαραίτητες γνώσεις, να ανακαλύψει ατέλειες που κάνουν τον εξυπηρετητή Ιστού ευάλωτο σε επιθέσεις. Πολλές εταιρίες χρησιμοποιούν τον Παγκόσμιο Ιστό ως ένα πεδίο προώθησης των προϊόντων τους. Κατασκευάζουν ηλεκτρονικές σελίδες, που προσομοιάζουν με εικονικά καταστήματα (τα λεγόμενα e-shops) και παρέχουν καταλόγους αγαθών και τιμών, καθώς και φόρμες προς συμπλήρωση με τα στοιχεία των πελατών. Το ηλεκτρονικό εμπόριο ήδη γνωρίζει μεγάλη διάδοση. Ο Παγκόσμιος Ιστός είναι μια από τις ευρύτερα χρησιμοποιούμενες εφαρμογές του Διαδικτύου. Ωστόσο, υπάρχουν σημαντικά προβλήματα ασφάλειας, που αφορούν τόσο στα προγράμματα πλοήγησης όσο και στους εξυπηρετητές Web.

Οι εξυπηρετητές Ιστού είναι πολύπλοκα και εξειδικευμένα προγράμματα, τα οποία δίνουν τη δυνατότητα στις σελίδες HTML (HyperText Markup Language) να καταστούν προσπελάσιμες από τα προγράμματα πλοήγησης, εφόσον υπάρχει σύνδεση του υπολογιστή με το Διαδίκτυο. Είναι, δηλαδή, σχεδιασμένοι να δέχονται ανώνυμες αιτήσεις από άγνωστους υπολογιστές σε όλο το Διαδίκτυο και να παραδίδουν τις ζητούμενες πληροφορίες γρήγορα και αποτελεσματικά. Δυστυχώς όμως δεν υπάρχει λογισμικό που η χρήση του να μην περικλείει κινδύνους και οι εξυπηρετητές Ιστού δεν αποτελούν εξαίρεση. Ένας εξυπηρετητής Ιστού μπορεί να ενσωματώνει προγράμματα στις ηλεκτρονικές σελίδες του. Τα προγράμματα αυτά δημιουργούνται με το πρωτόκολλο Common Gateway Interface (CGI) και ονομάζονται CGI scripts. Τα CGI scripts που εκτελούνται στην πλευρά του εξυπηρετητή κάθε φορά που κάποιος θέλει να συνδεθεί με αυτόν, μπορεί να είναι εξαιρετικά απλά, όπως για παράδειγμα ένας μετρητής που αυξάνει κάθε φορά που κάποιος επισκέπτεται τη σελίδα ή αρκετά πολύπλοκα, όπως για παράδειγμα αυτά που παρέχουν τη δυνατότητα για αγορά προϊόντων ή άλλες οικονομικές συναλλαγές μέσα από τον Παγκόσμιο Ιστό. Στον εξυπηρετητή Ιστού περιέχονται ο κατάλογος ρίζας (root directory) και η ρίζα εγγραφών (document root). Στη ρίζα εγγραφών φυλάσσονται οι αιτούμενες ιστοσελίδες του εξυπηρετητή. Τοποθετούνται εκεί, ώστε να υπάρχει πρόσβαση σε αυτές από το Διαδίκτυο. Στον κατάλογο ρίζας βρίσκονται τα αρχεία που ρυθμίζουν τις λειτουργίες του εξυπηρετητή και τα αρχεία CGI.

7.1.1 Η ΠΟΛΙΤΙΚΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για την ασφάλεια του εξυπηρετητή Ιστού και κατ' επέκταση για την ασφάλεια όλου του δικτύου, πρέπει να υπάρχει ένα ολοκληρωμένο σύστημα προστασίας. Η υλοποίηση του ανατίθεται στο διαχειριστή του εξυπηρετητή. Το σύστημα ασφάλειας ουσιαστικά δεν είναι τίποτα άλλο παρά μία περίληψη του πως πρέπει να λειτουργεί ο εξυπηρετητής ιστού, ώστε να

ανταποκρίνεται στις απαιτήσεις των χρηστών του. Για την κατασκευή ενός ασφαλούς εξυπηρετητή Ιστού σε οποιαδήποτε πλατφόρμα, πρέπει να ληφθούν υπόψη τα εξής θέματα [Πομ03]:

- ☑ Οι χρήστες του δικτύου δεν πρέπει σε καμία περίπτωση να μπορούν να εκτελούν προγράμματα ή εντολές κελύφους στον υπολογιστή όπου στεγάζεται ο εξυπηρετητής.

- ☑ Τα CGI scripts που τρέχουν στον εξυπηρετητή πρέπει να είναι ελεγμένα διεξοδικά ώστε να επιτελούν τη λειτουργία για την οποία προορίζονται

- ☑ Στην περίπτωση που ο εξυπηρετητής δεχθεί επίθεση, ο επιτιθέμενος δεν θα πρέπει να είναι σε θέση να τον χρησιμοποιήσει για να εξαπολύσει επιθέσεις εναντίον των υπόλοιπων υπολογιστών του δικτύου.

Το καθένα από τα παραπάνω απαιτεί τη λήψη ιδιαίτερων μέτρων. Δυστυχώς, κάποια από τα μέτρα που λαμβάνονται είναι αλληλοσυγκρουόμενα. Για παράδειγμα, για να ελαχιστοποιηθεί ο κίνδυνος της παρακολούθησης της επικοινωνίας πολλοί οργανισμοί αγοράζουν ασφαλείς εξυπηρετητές Web, που βασίζονται σε κρυπτογραφικά πρωτοκόλλα. Αλλά τέτοιοι εξυπηρετητές απαιτούν ψηφιακά υπογεγραμμένα πιστοποιητικά για να λειτουργήσουν και τα πιστοποιητικά αυτά πρέπει να ανανεώνονται τακτικά γεγονός που καθιστά τους εξυπηρετητές ευάλωτους στις λεγόμενες επιθέσεις «άρνησης υπηρεσίας» (Denial of Service attacks – DoS). Οι επιθέσεις «άρνησης υπηρεσίας» σχεδιάστηκαν με σκοπό να καταστήσουν τον υπολογιστή ή το δίκτυο ανίκανο να επιτελέσει τις συνηθισμένες του λειτουργίες. Συνήθως έχουν ως στόχο το εύρος ζώνης ή τη σύνδεση του δικτύου, όπου ανήκει ο υπολογιστής. Οι επιθέσεις με στόχο το εύρος ζώνης κατακλύζουν το δίκτυο με τόσο φόρτο που οι διαθέσιμες πηγές του ξοδεύονται και οι αιτήσεις των χρηστών δεν ικανοποιούνται. Οι επιθέσεις στη σύνδεση κατακλύζουν το δίκτυο με μεγάλο αριθμό αιτήσεων για σύνδεση, με αποτέλεσμα οι διαθέσιμες πηγές του συστήματος να καταναλώνονται και το σύστημα να μη μπορεί πλέον να ικανοποιήσει τις νόμιμες αιτήσεις των χρηστών του.

Η πολιτική της ασφάλειας, που θα εφαρμοστεί, για την υλοποίηση του συστήματος προστασίας είναι καλό να συμπεριλάβει και παράγοντες όπως:

- 🕮 Ποιοι επιτρέπεται να χρησιμοποιούν το σύστημα.
- 🕮 Πότε επιτρέπεται να το χρησιμοποιούν.
- 🕮 Τι επιτρέπεται να κάνουν.

Είναι πιθανό διαφορετικές ομάδες χρηστών να έχουν διαφορετικά δικαιώματα εισόδου στα διάφορα μέρη του εξυπηρετητή ιστού. Επίσης, οι διαδικασίες παροχής εισόδου στο σύστημα και οι διαδικασίες ανάκλησης της εισόδου, όταν για παράδειγμα ένας χρήστης φεύγει από το σύστημα, αποτελούν ένα σημαντικό κομμάτι του συστήματος προστασίας. Ένα ακόμη σημείο το οποίο πρέπει να ληφθεί υπόψη είναι το πώς ορίζεται η αποδεκτή χρήση του συστήματος. Ακόμη στο σύστημα προστασίας, πρέπει να συμπεριληφθούν οι μέθοδοι εισόδου (login) σε αυτό, τόσο για τους εσωτερικούς όσο και για τους εξωτερικούς χρήστες. Τέλος, ιδιαίτερο βάρος πρέπει να δοθεί στα πρωτόκολλα που αφορούν στις αντιδράσεις του συστήματος σε τυχόν κενά ασφαλείας.

Τελικά, τόσο οι χρήστες του Διαδικτύου όσο και οι διαχειριστές των εξυπηρετών Ιστού έχουν λόγους να ανησυχούν για την ασφάλεια των δεδομένων που μεταφέρονται μέσω του

δικτύου. Το πρωτόκολλο επικοινωνίας TCP/IP (Transfer Control Protocol/Internet Protocol) δεν έλαβε υπόψη θέματα ασφάλειας δικτύου κατά το σχεδιασμό του. Αυτό έχει ως αποτέλεσμα να δημιουργούνται προβλήματα ασφάλειας στη μετάδοση εμπιστευτικών εγγράφων από τον εξυπηρετητή προς στο πρόγραμμα πλοήγησης του χρήστη ή ακόμη και στην αποστολή προσωπικών πληροφοριών του χρήστη πίσω στον εξυπηρετητή

Ακολούθως αναφέρονται ορισμένα συγκεκριμένα παραδείγματα όσον αφορά την πολιτική ασφάλειας των προγραμμάτων πλοήγησης (web browsers) και των εξυπηρετητών ιστού (web servers):

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΠΛΟΗΓΗΣΗΣ

Οι χρήστες πρέπει να χρησιμοποιούν το λογισμικό αναζήτησης πληροφορίας από το διαδίκτυο αποκλειστικά για τις ανάγκες της επιχείρησης. Οποιαδήποτε προσωπική χρήση του λογισμικού ανεύρεσης πληροφορίας δεν πρέπει:

- Να παρεμποδίζει τις κανονικές δραστηριότητες της επιχείρησης.
- Να σχετίζεται με κερδοσκοπικές ενέργειες που δεν εντάσσονται στις δραστηριότητες της επιχείρησης.
- Να εκθέτει και να επηρεάζει αρνητικά την φήμη και την εικόνα της επιχείρησης.

Απαγορεύεται η επίσκεψη σε δικτυακές τοποθεσίες (sites) που περιέχουν υβριστικές ή ανήθικες πληροφορίες. Όταν υπάρχει υποψία ότι κάποιος χρήστης παραβιάζει τις οδηγίες χρήσης του Παγκόσμιου Ιστού τότε οι κινήσεις του θα πρέπει να καταγράφονται προκειμένου να ληφθούν περαιτέρω μέτρα. Οι εξυπηρετητές Ιστού θα πρέπει να καταγράφουν ης επισκέψεις σε οποιοδήποτε ιστότοπο. Οι χρήστες θα πρέπει να είναι ενήμεροι ότι οι εξυπηρετητές ιστού καταγράφουν τις επισκέψεις σε οποιοδήποτε ιστότοπο. Ο διαχειριστής δικτύου θα πρέπει να δώσει στους χρήστες λίστα με τα Uniform Resource Locators-URLs που περιέχουν ρατσιστικό ή ανήθικο περιεχόμενο. Το λογισμικό του Παγκόσμιου Ιστού θα πρέπει να διαμορφωθεί έτσι ώστε να απαγορεύει τις επισκέψεις σε αυτούς τους ιστότοπους.

Οι εξυπηρετητές Ιστού θα πρέπει να διαμορφωθούν έτσι ώστε:

- Η πρόσβαση στο Διαδίκτυο να γίνεται μόνο μέσω firewall-http proxy server.
- Να εξετάζουν οποιοδήποτε αρχείο αντλείται από το Διαδίκτυο προκειμένου να εντοπίσουν τυχόν ιομορφικό λογισμικό.
- Να απαγορεύουν επισκέψεις σε ιστότοπους που περιέχουν υλικό σεξουαλικού ή ρατσιστικού περιεχομένου.
- Τα προγράμματα Java, JavaScript, ή ActiveX να αντλούνται μόνο έπειτα από έγκριση της διεύθυνσης της επιχείρησης.

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΞΥΠΗΡΕΤΗΤΩΝ ΙΣΤΟΥ

Απαγορεύεται οι χρήστες να εγκαθιστούν ή να αντλούν από το Διαδίκτυο λογισμικό για τον εξυπηρετητή Ιστού. Η χρήση μη εγκεκριμένου λογισμικού για τον εξυπηρετητή Ιστού αποτελεί παραβίαση της πολιτικής ασφαλείας και επομένως επιβάλλεται να αποδοθούν ευθύνες. Καμία εμπιστευτική πληροφορία δεν θα πρέπει να είναι διαθέσιμη από το ιστοχώρο (web site). Το λογισμικό του εξυπηρετητή θα πρέπει να εγκριθεί από τον υπεύθυνο διαχείρισης. Προκειμένου να εγκριθεί η δομή και το περιεχόμενο των web σελίδων θα πρέπει να ακολουθηθεί η σχετική διαδικασία έγκρισης όπως γίνεται και με όλα τα έντυπα της

επιχείρησης. Προτού επιτραπεί ανοικτή πρόσβαση θα πρέπει να έχει ολοκληρωθεί η κατασκευή των web σελίδων και επίσης θα πρέπει να πιστοποιηθεί ότι όλες οι συνδέσεις δουλεύουν όπως αναμενόταν. Οποιεσδήποτε ιστοσελίδες είναι υπό κατασκευή δε θα πρέπει να εμφανίζονται στους ιστοχώρους της επιχείρησης. Δεν θα πρέπει να γίνεται έλεγχος από μακριά του εξυπηρετητή. Όλες οι λειτουργίες διαχείρισης θα πρέπει να γίνονται από την κονσόλα. Η εισερχόμενη HTTP (Hyper Text Transfer Protocol) κίνηση θα πρέπει να ελέγχεται αυστηρά για ιομορφικό λογισμικό. Όταν υπάρχει υποψία ότι κάποιος χρήστης παραβιάζει τις οδηγίες χρήσης του εξυπηρετητή Ιστού τότε οι κινήσεις του θα πρέπει να καταγράφονται προκειμένου να ληφθούν περαιτέρω μέτρα. Ευαίσθητη, εμπιστευτική ή ιδιωτική πληροφορία δεν θα πρέπει να αποθηκεύεται στον εξωτερικό εξυπηρετητή.

7.1.2 ΥΛΟΠΟΙΗΣΗ ΑΣΦΑΛΕΣ ΔΙΚΤΥΟΥ ΓΙΑ ΕΝΑΝ ΕΞΥΠΗΡΕΤΗΤΗ ΙΣΤΟΥ (WEB SERVER)

Η υποδομή του δικτύου που υποστηρίζει τον εξυπηρετητή διαδραματίζει έναν κρίσιμο ρόλο στην ασφάλεια του εξυπηρετητή [NIST 800-44]. Στις περισσότερες διαμορφώσεις, η υποδομή δικτύων είναι η πρώτη γραμμή υπεράσπισης μεταξύ του Διαδικτύου και ενός δημόσιου εξυπηρετητή. Αν και οι εκτιμήσεις της υποδομής δικτύου επηρεάζονται από πολλούς παράγοντες εκτός από την ασφάλεια (π.χ., κόστος, απόδοση, και αξιοπιστία), αυτό το τμήμα θα αντιμετωπίσει πρώτιστα τα ζητήματα ασφάλειας. Ωστόσο το σχέδιο δικτύων από μόνο του δεν μπορεί να προστατεύσει έναν εξυπηρετητή. Η συχνότητα, η εκλέπτυνση, ακόμη και η ποικιλία των επιθέσεων Ιστού που διαπράττονται σήμερα υποστηρίζουν την ιδέα ότι η ασφάλεια Ιστού πρέπει να είναι εφαρμοσμένη μέσω των στρώσεων και των διαφορετικών αμυντικών μηχανισμών (Defense In Depth). Αυτό το τμήμα συζητά εκείνα τα τμήματα των δικτύων που μπορούν να υποστηρίξουν και να προστατεύσουν τους εξυπηρετητές για περαιτέρω ενίσχυση της γενικής τους ασφάλειάς.

Ένας οργανισμός έχει πολλές επιλογές κατά τη διάρκεια της επιλογής μιας τοποθεσίας δικτύωσης και η ασφάλεια θα πρέπει να είναι ο κύριος παράγοντας στην απόφαση μεταξύ εκείνων των επιλογών. Η τοποθεσία δικτύων είναι η πρώτη και μεταξύ άλλων η κρισιμότερη απόφαση δικτύωσης που έχει επιπτώσεις στην ασφάλεια των εξυπηρετητών. Η τοποθεσία δικτύου είναι σημαντική για διάφορους λόγους. Η τοποθεσία δικτύων καθορίζει ποια υποδομή δικτύου μπορεί να χρησιμοποιηθεί για να προστατεύσει τον εξυπηρετητή. Παραδείγματος χάριν, εάν ο εξυπηρετητής του οργανισμού βρίσκεται πίσω από ένα φράγμα ασφάλειας (Firewall), τότε το φράγμα ασφάλειας δεν μπορεί να χρησιμοποιηθεί για να ελέγξει την κυκλοφορία προς και από το εσωτερικό δίκτυο η τον εξυπηρετητή. Η θέση δικτύων καθορίζει επίσης ποια άλλα τμήματα του δικτύου είναι τρωτά όταν ο εξυπηρετητής είναι εκτεθειμένος. Παραδείγματος χάριν, εάν ο εξυπηρετητής βρίσκεται στο εσωτερικό δίκτυο, τότε το εσωτερικό δίκτυο είναι αίτιο επίθεσης από τον εκτεθειμένο εξυπηρετητή.

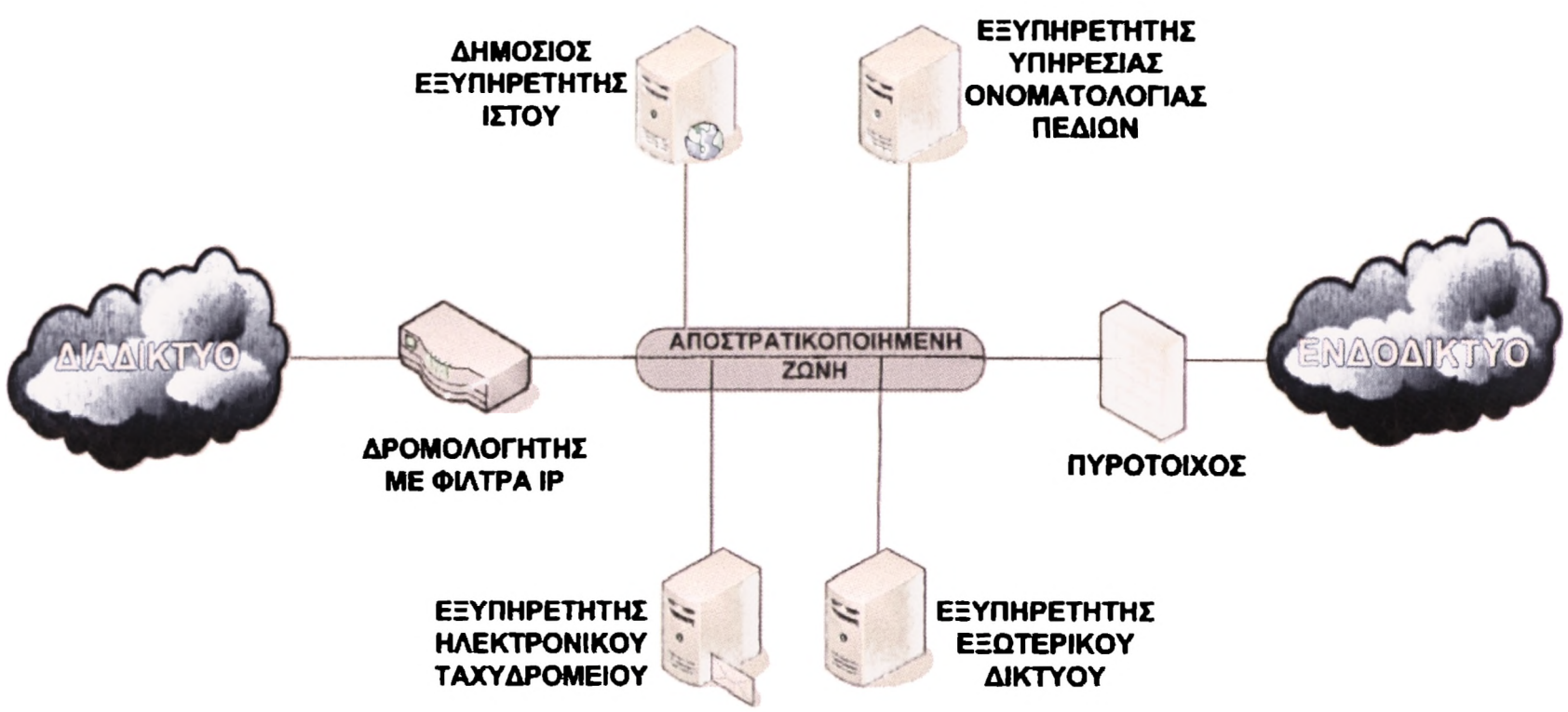
Ένας οργανισμός μπορεί να επιλέξει να μην τοποθετήσει έναν εξυπηρετητή στο δίκτυό του αλλά να μεταφέρει την «φιλοξενία» σε μια Τρίτη Οντότητα (Third Party).

7.1.2.1 ΑΠΟΣΤΡΑΤΙΚΟΠΟΙΗΜΕΝΗ ΖΩΝΗ (DMZ)

Μια αποστρατικοποιημένη ζώνη (DMZ) μπορεί να οριστεί ως ένα τμήμα υπολογιστών

(hosts) ή δικτύων που παρεμβάλλεται ως μια "ουδέτερη ζώνη" μεταξύ του ιδιωτικού δικτύου ενός οργανισμού και του Διαδικτύου. Αποτρέπει τους χρήστες του εξυπηρετητή από το να έχουν άμεση πρόσβαση στο εσωτερικό δίκτυο ενός οργανισμού (Intranet). Μια αποστρατικοποιημένη ζώνη μετριάζει τους κινδύνους της τοποθέτησης ενός εξυπηρετητή σε ένα εσωτερικό δίκτυο ή της έκθεσής του άμεσα στο Διαδίκτυο. Αυτή είναι μια λύση συμβιβασμού που προσφέρει περισσότερα οφέλη με το λιγότερο ποσοστό κινδύνου για τους περισσότερους οργανισμούς. Η αποστρατικοποιημένη ζώνη επιτρέπει την πρόσβαση στους πόρους που είναι τοποθετημένοι μέσα σε αυτή τόσο στους εσωτερικούς όσο και στους εξωτερικούς χρήστες. Υπάρχει μια ευρεία ποικιλία διαμορφώσεων των αποστρατικοποιημένων ζωνών, κάθε μια με τα πλεονεκτήματά της και τις αδυναμίες της.

Στη δημιουργία μιας αποστρατικοποιημένης ζώνης ένας οργανισμός τοποθετεί ένα πυρότοιχο (Firewall) μεταξύ του δρομολογητή της και του εσωτερικού δικτύου (σε μερικές διαμορφώσεις ο ίδιος ο δρομολογητής μπορεί να ενεργήσει ως βασικός πυρότοιχος – Firewall). Το σχήμα 7-1 επεξηγεί ένα παράδειγμα μιας απλής αποστρατικοποιημένης ζώνης (DMZ) η οποία χρησιμοποιεί έναν δρομολογητή με Λίστες Ελέγχου Πρόσβασης (ACLs) για να περιορίσουν ορισμένους τύπους δικτυακής κυκλοφορίας από και προς την αποστρατικοποιημένη ζώνη.

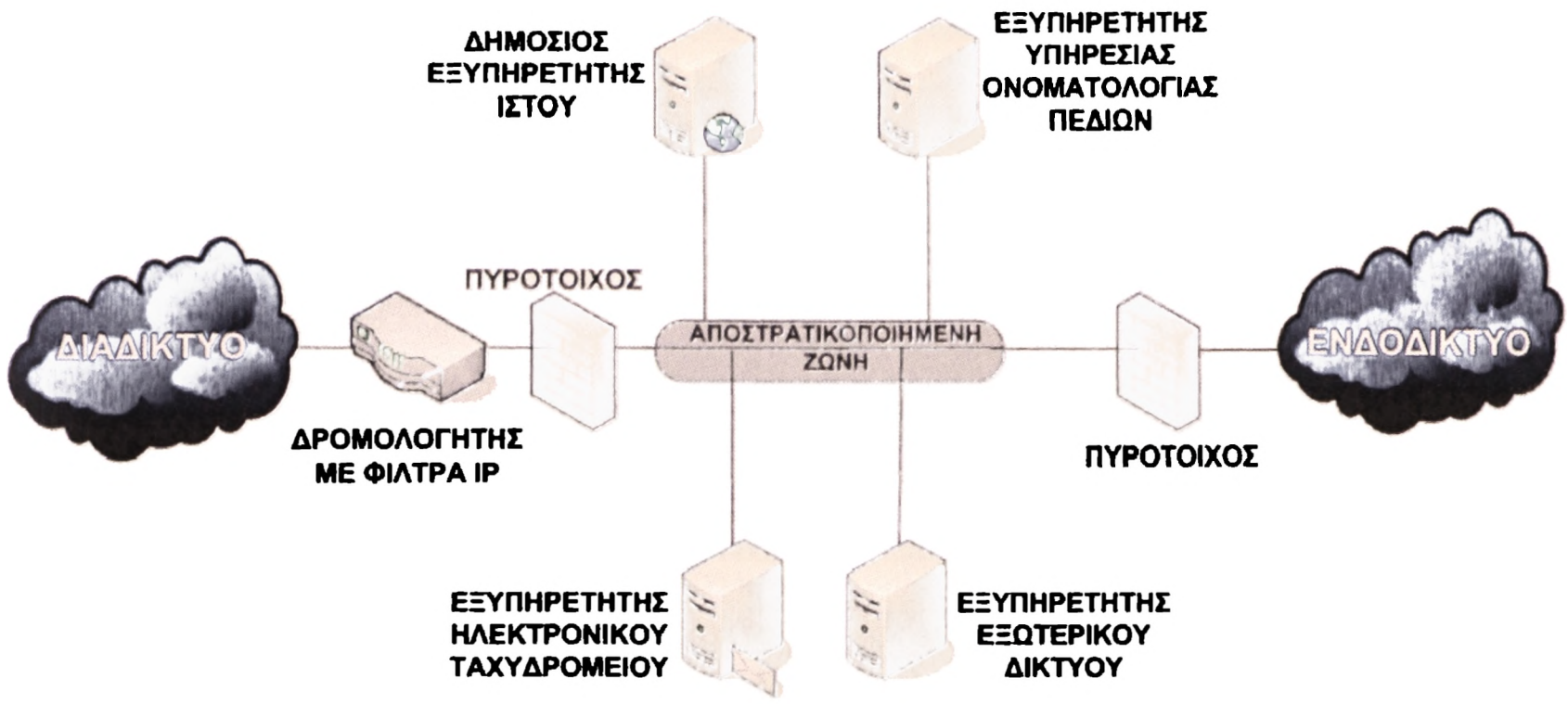


Σχήμα 7-1: Βασική Αποστρατικοποιημένη Ζώνη

Αυτός ο τύπος της αποστρατικοποιημένης ζώνης είναι μια προσέγγιση χαμηλού κόστους. Αυτός ο τύπος αποστρατικοποιημένης ζώνης είναι κατάλληλος μόνο για μικρές οργανώσεις που αντιμετωπίζουν ελάχιστες απειλές. Η βασική αδυναμία αυτής της προσέγγισης είναι ότι ενώ ο δρομολογητής είναι σε θέση να προστατεύσει το δίκτυο από τις περισσότερες επιθέσεις δικτύων, δεν «αναγνωρίζει» το HTTP και γι'αυτό το λόγο δεν μπορεί να προστατεύσει από τις επιθέσεις του στρώματος εφαρμογής που στοχεύουν τον εξυπηρετητή.

Μια ανώτερη προσέγγιση είναι να προστεθεί ένας δεύτερος πυρότοιχος (Firewall) μεταξύ του Διαδικτύου και της αποστρατικοποιημένης ζώνης. Αυτό προσφέρει την καλύτερη

προστασία στην αποστρατικοποιημένη ζώνη. Ένα παράδειγμα αυτού του τύπου υλοποίησης δικτύου φαίνεται στο παρακάτω σχήμα (σχήμα 7-2).

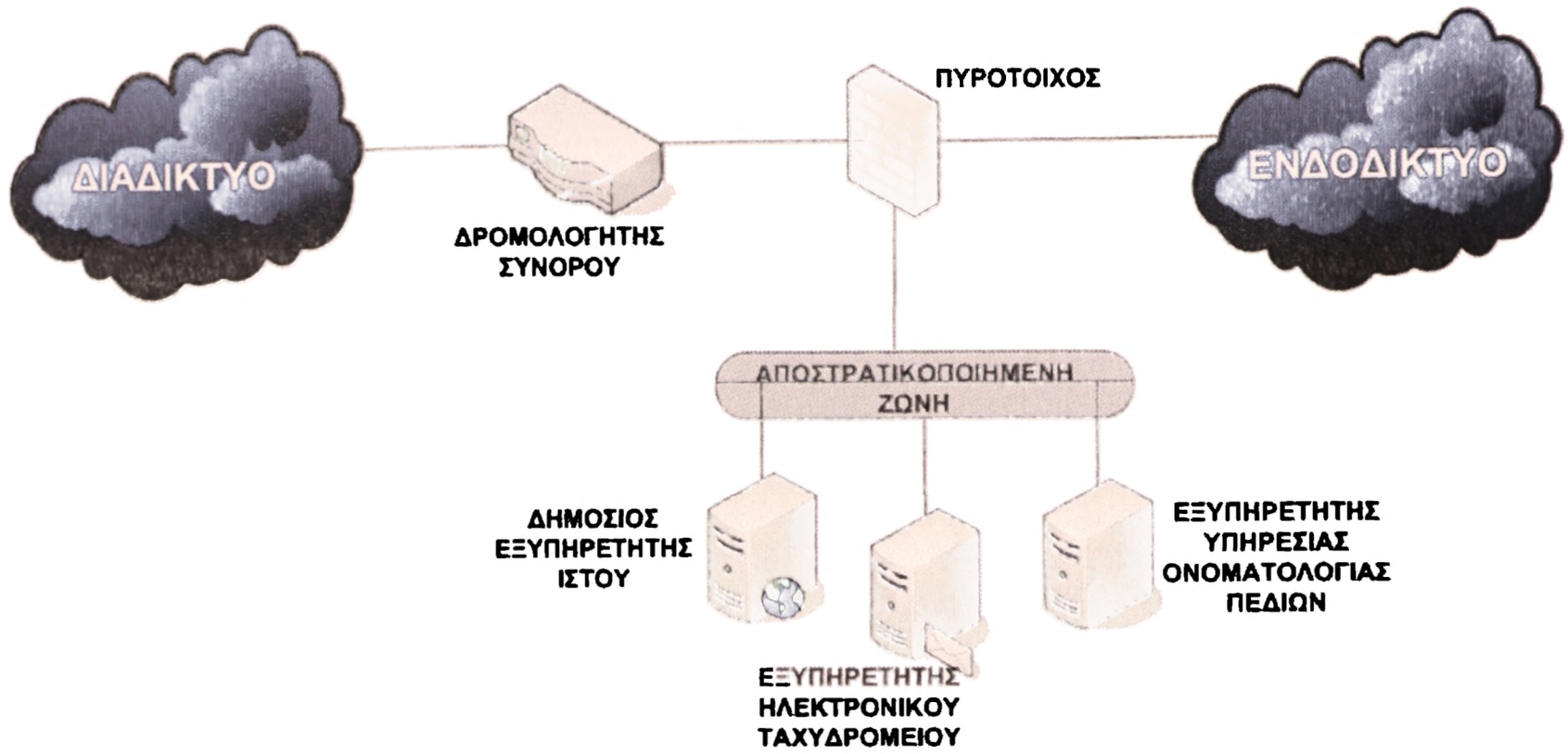


Σχήμα 7-2: Αποστρατικοποιημένη ζώνη με δύο πυρότοιχους (firewalls)

Αυτός ο τύπος αποστρατικοποιημένης ζώνης με δύο πυρότοιχους προσφέρει ανώτερη προστασία σε ένα δρομολογητή βασισμένο στην αποστρατικοποιημένη ζώνη αφού οι πυρότοιχοι μπορούν να θέσουν έναν πιο σύνθετο και ισχυρό κανόνα ασφάλειας. Επιπλέον, ο πυρότοιχος είναι συχνά ικανός να αναλύσει την εισερχόμενη και εξερχόμενη κυκλοφορία HTTP και μπορεί να ανιχνεύσει και να προστατεύσει ενάντια στις επιθέσεις του στρώματος εφαρμογής που στοχεύουν στον εξυπηρετητή Ιστού. Ανάλογα με τη διαμόρφωση των πυρότοιχων και το επίπεδο κυκλοφορίας που λαμβάνει η αποστρατικοποιημένη ζώνη, μπορεί να οδηγήσει σε μερικά ζητήματα απόδοσης. Για τους οργανισμούς που επιθυμούν την ασφάλεια των δύο πυρότοιχων αλλά που δεν έχουν τους πόρους για να τα αποκτήσουν, υπάρχει μια άλλη επιλογή αποκαλούμενη «service leg» DMZ. Σε αυτήν την διαμόρφωση, ένας πυρότοιχος κατασκευάζεται με τρεις (ή περισσότερες) διεπαφές δικτύων. Μια διεπαφή δικτύων συνδέεται με το δρομολογητή, μια άλλη διεπαφή συνδέεται με το εσωτερικό δίκτυο και μια τρίτη διεπαφή δικτύων συνδέεται με την αποστρατικοποιημένη ζώνη.

Αυτή η διαμόρφωση υποβάλλει τον πυρότοιχο σε έναν αυξανόμενο κίνδυνο υποβάθμισης των υπηρεσιών κατά τη διάρκεια μιας επίθεσης «άρνησης υπηρεσιών» που στοχεύει στον εξυπηρετητή Ιστού. Σε μια τυποποιημένη διαμόρφωση δικτύων αποστρατικοποιημένης ζώνης (που συζητείται παραπάνω), μια επίθεση «άρνησης υπηρεσιών»" (DoS) ενάντια στον εξυπηρετητή Ιστού γενικά έχει επιπτώσεις μόνο σε αυτόν . Σε μια διαμόρφωση δικτύου αποστρατικοποιημένης ζώνης τύπου «service leg», το φράγμα ασφάλειας αντέχει την ορμή οποιασδήποτε επίθεσης «άρνησης υπηρεσιών» επειδή πρέπει να εξετάσει οποιαδήποτε κυκλοφορία δικτύων πριν η κυκλοφορία αυτή φθάσει στον εξυπηρετητή ιστού (ή οποιοδήποτε άλλο DMZ ή στους πόρους του εσωτερικού δικτύου).

Ένα τέτοιο παράδειγμα υλοποίησης φαίνεται στο παρακάτω σχήμα (σχήμα 7-3).



Σχήμα 7-3: Αποστρατικοποιημένη ζώνη με πυρότοιχο (firewall) τριών διεπαφών

Τα πλεονεκτήματα μιας αποστρατικοποιημένης ζώνης (DMZ) από τη σκοπιά της ασφάλειας είναι τα εξής [NIST 800-44]

- ☺ Ο εξυπηρετητής ιστού μπορεί να προστατευθεί καλύτερα και η δικτυακή κυκλοφορία από και προς τον εξυπηρετητή μπορεί να ελεγχθεί.
- ☺ Η έκθεση του εξυπηρετητή ιστού δεν απειλεί άμεσα την εσωτερική παραγωγή του δικτύου.
- ☺ Μεγαλύτερος έλεγχος μπορεί να παρασχεθεί όσον αφορά την ασφάλεια του εξυπηρετητή ιστού αφού η κυκλοφορία από και προς τον εξυπηρετητή ιστού μπορεί να ελεγχθεί.
- ☺ Η διαμόρφωση δικτύων αποστρατικοποιημένης ζώνης μπορεί να βελτιστοποιηθεί για να υποστηρίξει και να προστατεύσει τους εξυπηρετητές ιστού.

Τα μειονεκτήματα μιας αποστρατικοποιημένης ζώνης (DMZ) από την σκοπιά της ασφάλειας είναι τα εξής:

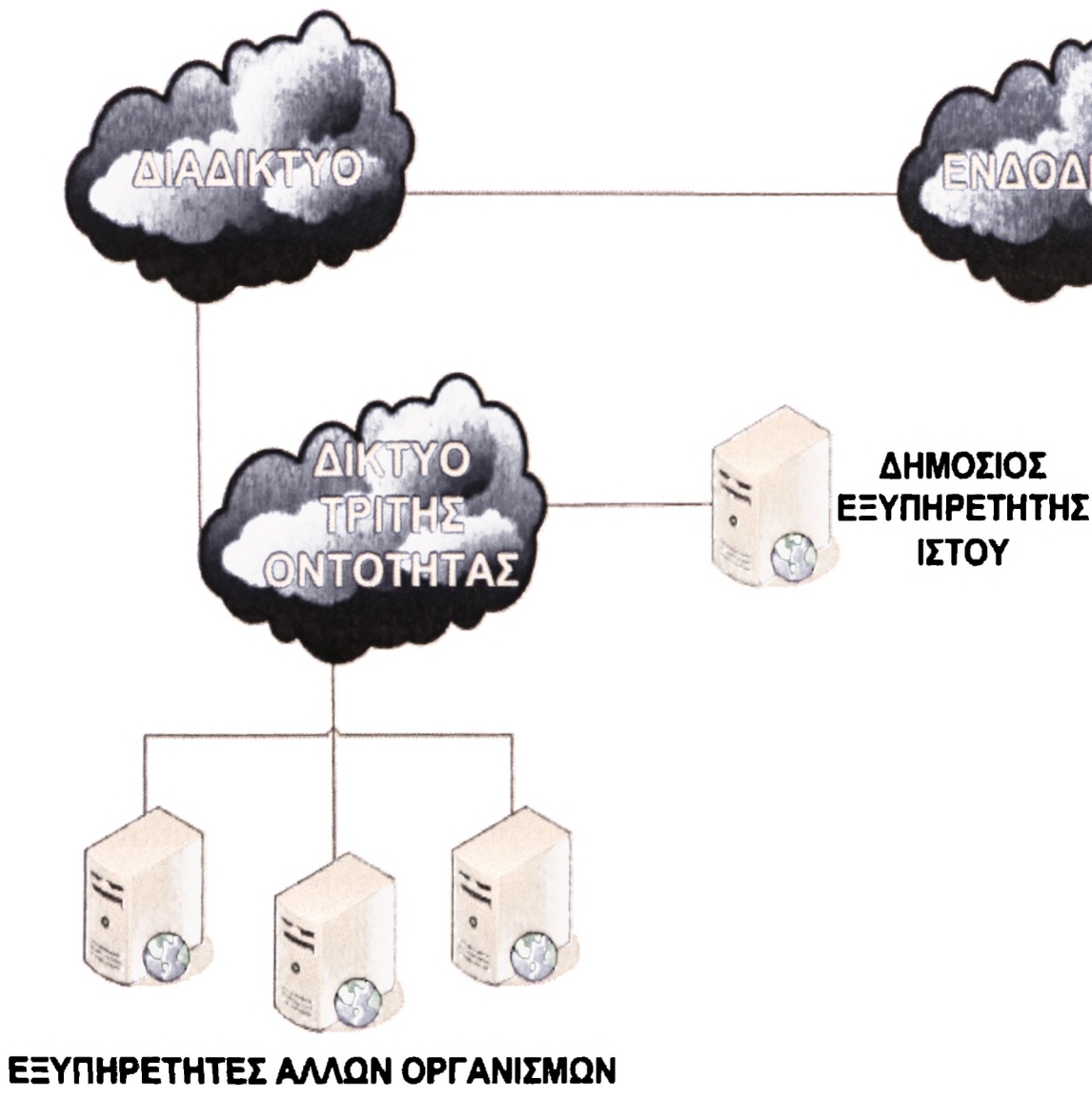
- ☹ Οι επιθέσεις «άρνησης υπηρεσιών» που στοχεύουν στον εξυπηρετητή Ιστού μπορούν να έχουν επίδραση και στο εσωτερικό δίκτυο.
- ☹ Ανάλογα με την κυκλοφορία που επιτρέπεται από και προς την αποστρατικοποιημένη ζώνη και το εσωτερικό δίκτυο, είναι πιθανόν ότι ο εξυπηρετητής ιστού μπορεί να χρησιμοποιηθεί για επίθεση ή για να εκθέσει τους οικοδεσπότες (hosts) στο εσωτερικό δίκτυο.

7.1.2.2 «ΜΕΤΑΦΕΡΟΜΕΝΗ» ΦΙΛΟΞΕΝΙΑ

Πολλοί οργανισμοί επιλέγουν να μεταφέρουν τη «φιλοξενία» του εξυπηρετητή τους σε μια Τρίτη Οντότητα (π.χ ένας φορέας παροχής υπηρεσιών Διαδικτύου-ISP, υπηρεσίες

«φιλοξενίας» του Ιστού, ή άλλη κυβερνητική αντιπροσωπεία). Σε αυτή την περίπτωση, ο εξυπηρετητής δεν τοποθετείται στο δίκτυο του οργανισμού. Το δίκτυο που προσφέρει την υπηρεσία της «φιλοξενίας» έχει ένα αφιερωμένο δίκτυο το οποίο «φιλοξενεί» πολλούς εξυπηρετητές (για πολλούς οργανισμούς/επιχειρήσεις) οι οποίοι λειτουργούν σε ένα απλό δίκτυο.

Στο παρακάτω σχήμα (σχήμα 7-4) φαίνεται η εξωτερική «φιλοξενία» ενός εξυπηρετητή Ιστού.



Σχήμα 7-4: Εξωτερική «φιλοξενία» ενός εξυπηρετητή Ιστού

Τα πλεονεκτήματα της μεταφοράς της «φιλοξενίας» από τη σκοπιά της ασφάλειας είναι τα ακόλουθα:

- ☺ Οι επιθέσεις "άρνησης υπηρεσιών" που στοχεύουν στον web εξυπηρετητή δεν έχουν καμία επίδραση στο δίκτυο του οργανισμού.
- ☺ Η έκθεση του εξυπηρετητή δεν απειλεί άμεσα το εσωτερικό δίκτυο.
- ☺ Η Τρίτη Οντότητα στην οποία θα ανατεθεί η «φιλοξενία» του εξυπηρετητή μπορεί να έχει μεγαλύτερη γνώση στην ασφάλεια και την προστασία των εξυπηρετητών.
- ☺ Το δίκτυο μπορεί να βελτιστοποιηθεί μόνο για την υποστήριξη και την προστασία των εξυπηρετητών.

Τα μειονεκτήματα της μεταφοράς της «φιλοξενίας» από τη σκοπιά της ασφάλειας είναι τα ακόλουθα:

- ☹ Είναι δύσκολη η εξ αποστάσεως διαχείριση του εξυπηρετητή καθώς επίσης και η εξ αποστάσεως αναπροσαρμογή (update) του λογισμικού (software) και του υλικού (hardware) του εξυπηρετητή.
- ☹ Ελάχιστος έλεγχος μπορεί να παρασχεθεί όσον αφορά την ασφάλειας του εξυπηρετητή.
- ☹ Ο εξυπηρετητής μπορεί να επηρεασθεί από επιθέσεις που στοχεύουν σε άλλους εξυπηρετητές οι οποίοι «φιλοξενούνται» στο ίδιο δίκτυο από μια Τρίτη Οντότητα.

7.2 IPSec

Το 1994, το Συμβούλιο Αρχιτεκτονικής Διαδικτύου (Internet Architecture Board -IAB) έκδωσε μία έκθεση με τίτλο *Ασφάλεια στην Αρχιτεκτονική του Διαδικτύου* (RFC 1636). Η έκθεση δήλωνε τη γενική ομοφωνία πως το Διαδίκτυο χρειάζεται περισσότερη και καλύτερη ασφάλεια και προσδιόρισε περιοχές κλειδιά για τους μηχανισμούς ασφαλείας. Μεταξύ αυτών ήταν η ανάγκη να ασφαλιστεί η υποδομή του δικτύου από μη εξουσιοδοτημένη παρακολούθηση και έλεγχο της κίνησης δικτύου, όπως επίσης και η ανάγκη να ασφαλιστεί η κίνηση τερματικού χρήστη προς τερματικό χρήστη χρησιμοποιώντας πιστοποίηση και μηχανισμούς κρυπτογράφησης.

Αυτά τα ενδιαφέροντα είναι πλήρως δικαιολογημένα. Ως επιβεβαίωση, η ετήσια έκθεση του 1998 από την Computer Emergency Response Team (CERT) καταγράφει περισσότερα από 1300 αναφερθέντα περιστατικά ασφαλείας που επηρέασαν σχεδόν 20,000 τοποθεσίες (sites) [Site4]. Οι περισσότερο σημαντικοί τύποι επιθέσεων περιλάμβαναν εξαπάτηση IP, στις οποίες οι προσβολείς δημιούργησαν πακέτα με ψεύτικες διευθύνσεις IP και εκμεταλλεύτηκαν εφαρμογές που χρησιμοποιούν πιστοποίηση βασισμένη στη διεύθυνση IP, διάφορες μορφές κρυφακούσματος και αναρρόφηση πακέτων, στις οποίες οι επιτιθέμενοι διάβασαν μεταδομένη πληροφορία, περιλαμβάνοντας πληροφορία logon και περιεχόμενα βάσεων δεδομένων.

Σε απόκριση σε αυτά τα ζητήματα, το Συμβούλιο Αρχιτεκτονικής Διαδικτύου περιέλαβε την πιστοποίηση και την κρυπτογράφηση ως απαραίτητα χαρακτηριστικά ασφαλείας στο IP επόμενης γενεάς, το οποίο έχει εκδοθεί ως IPv6. Ευτυχώς, αυτές οι δυνατότητες ασφαλείας σχεδιάστηκαν για να είναι χρησιμοποιήσιμες τόσο με το IPv4 όσο και με το IPv6. Αυτό σημαίνει ότι οι κατασκευαστές μπορούν να ξεκινήσουν να προσφέρουν αυτά τα χαρακτηριστικά τώρα και πολλοί κατασκευαστές έχουν ήδη κάποια δυνατότητα IPSec στα προϊόντα τους.

7.2.1 ΕΦΑΡΜΟΓΕΣ ΤΟΥ IPSec

Το IPSec παρέχει τη δυνατότητα να ασφαλίζει τις επικοινωνίες κατά μήκος ενός τοπικού δικτύου, κατά μήκος ιδιωτικών και δημόσιων δικτύων ευρείας περιοχής και κατά μήκος του Διαδικτύου. Παραδείγματα της χρήσης του περιλαμβάνουν τα ακόλουθα [Stall00]:

- **Ασφάλιση συνδεσιμότητας υποκαταστημάτων πάνω στο Διαδίκτυο:** Μία εταιρεία μπορεί να οικοδομήσει ένα ασφαλές νοητό ιδιωτικό δίκτυο πάνω από το Δια

δίκτυο ή πάνω από κάποιο δημόσιο δίκτυο ευρείας περιοχής. Αυτό επιτρέπει σε μία επιχείρηση να βασίζεται ισχυρά στο Διαδίκτυο μειώνοντας την ανάγκη της για ιδιωτικά δίκτυα, γλιτώνοντας κόστος και επιβάρυνση διαχείρισης δικτύου.

- **Ασφαλή απομακρυσμένη πρόσβαση πάνω στο Διαδίκτυο:** Ένας τερματικός χρήστης του οποίου το σύστημα είναι εφοδιασμένο με πρωτόκολλα ασφαλείας IP μπορεί να κάνει μία τοπική κλήση σε έναν παροχέα υπηρεσίας Διαδικτύου (ISP) και να επιτύχει ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο. Αυτό μειώνει το κόστος των χρεώσεων διοδίων για τους ταξιδεύοντες εργαζόμενους.

- **Αποκατάσταση εξωδικτυακής και ενδοδικτυακής συνδεσιμότητας με συνεταίρους:** Το IPSec μπορεί να χρησιμοποιηθεί για να ασφαλίσει την επικοινωνία με άλλους οργανισμούς, εξασφαλίζοντας πιστοποίηση και εμπιστευτικότητα και παρέχοντας ένα μηχανισμό ανταλλαγής κλειδιού.

- **Εμπλουτισμός ασφάλειας ηλεκτρονικού εμπορίου:** Έστω και εάν κάποιες εφαρμογές του διαδικτύου και ηλεκτρονικού εμπορίου έχουν ενσωματωμένα πρωτόκολλα ασφαλείας, η χρήση του IPSec εμπλουτίζει αυτήν την ασφάλεια.

Το βασικό χαρακτηριστικό του IPSec που του επιτρέπει να υποστηρίζει αυτές τις ποικίλες εφαρμογές είναι ότι μπορεί να κρυπτογραφήσει και/ή να πιστοποιήσει όλη την κίνηση στο επίπεδο IP. Έτσι, μπορούν να ασφαλιστούν όλες οι κατανεμημένες εφαρμογές, συμπεριλαμβάνοντας το απομακρυσμένο logon, εφαρμογές πελάτη/εξυπηρετητή, ηλεκτρονικό ταχυδρομείο, μεταφορά αρχείων, πρόσβαση στο διαδίκτυο και ούτω καθεξής.

7.2.2 Ο ΣΚΟΠΟΣ ΤΟΥ IPSec

Το IPSec παρέχει τρεις κύριες ευκολίες: Μια λειτουργία μόνο πιστοποίησης αναφερόμενη ως Επικεφαλίδα Πιστοποίησης (Authentication Header-AH), μία συνδυασμένη λειτουργία πιστοποίησης/κρυπτογράφησης ονομαζόμενη Ενθυλακωμένο Φορτίο Ασφαλείας (Encapsulating Security Payload-ESP) και μία λειτουργία ανταλλαγής κλειδιού. Για τα νοητά ιδιωτικά δίκτυα, είναι συνήθως επιθυμητή τόσο η πιστοποίηση όσο και η κρυπτογράφηση, επειδή είναι σημαντικό και (1) να εξασφαλίζεται πως μη εξουσιοδοτημένοι χρήστες δε διαπερνούν το νοητό ιδιωτικό δίκτυο και (2) να εξασφαλίζεται πως αυτοί που κρυφακούν στο Διαδίκτυο δε μπορούν να διαβάσουν μηνύματα που αποστέλλονται πάνω στο νοητό ιδιωτικό διαδίκτυο. Επειδή και τα δύο χαρακτηριστικά είναι συνήθως επιθυμητά, οι περισσότερες υλοποιήσεις είναι πολύ πιθανό να χρησιμοποιούν το ESP παρά το AH. Η λειτουργία ανταλλαγής κλειδιού επιτρέπει τη χειροκίνητη ανταλλαγή κλειδιών όπως επίσης και ένα αυτοματοποιημένο σχήμα.

Η προδιαγραφή του IPSec είναι ιδιαίτερα πολύπλοκη και καλύπτει πολυάριθμα έγγραφα. Τα περισσότερο σημαντικά από αυτά, που εκδόθηκαν το Νοέμβριο του 1998 είναι οι RFCs 2401, 2402, 2406 και 2408.

7.2.3 ΣΧΕΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Μία βασική ιδέα που εμφανίζεται τόσο στους μηχανισμούς πιστοποίησης όσο και στους μηχανισμούς εμπιστευτικότητας για το IPSec είναι η Σχέση Ασφαλείας (Security Association-SA). Μία σχέση είναι μία μονόδρομη συγγένεια μεταξύ ενός αποστολέα και ενός παραλήπτη που παρέχει υπηρεσίες ασφαλείας στην κίνηση που μεταφέρεται πάνω σε αυτή. Εάν απαιτείται μία ομότιμη συγγένεια, για μία αμφίδρομη ασφαλή ανταλλαγή, τότε απαιτούνται δύο σχέσεις ασφαλείας. Οι υπηρεσίες ασφαλείας παρέχονται σε μία SA για τη χρήση των AH ή ESP, αλλά όχι και των δύο.

Μία σχέση ασφαλείας είναι μοναδικά προσδιορισμένη από τρεις παραμέτρους:

- **Κατάλογος παραμέτρων ασφαλείας (Security Parameters Index-SPI):** Μία σειρά bit εκχωρημένη σε αυτή την SA η οποία έχει μόνον τοπική σημασία. Ο SPI μεταφέρεται μέσα στις επικεφαλίδες AH και ESP για να επιτρέψει στο λαμβάνον σύστημα να επιλέξει τη SA κάτω από την οποία θα επεξεργάζεται ένα ληφθέν πακέτο.
- **Διεύθυνση προορισμού IP:** Επί του παρόντος, επιτρέπονται μόνο διευθύνσεις μονής αποστολής. Αυτή είναι η διεύθυνση του προοριζόμενου τερματικού σημείου της SA, η οποία μπορεί να είναι ένα σύστημα τερματικού χρήστη ή ένα σύστημα δικτύου όπως ένας τοίχος προστασίας (firewall) ή δρομολογητής.
- **Αναγνωριστής πρωτοκόλλου ασφαλείας:** Αυτός προσδιορίζει εάν η σχέση είναι μία σχέση ασφαλείας AH ή ESP.

Για το λόγο αυτό, σε κάθε πακέτο IP, η σχέση ασφαλείας είναι μοναδικά προσδιορισμένη από τη Διεύθυνση Προορισμού στην επικεφαλίδα IPv4 ή IPv6 και το SPI στην εσωκλεισμένη επικεφαλίδα επέκτασης (AH ή ESP).

7.2.4 ΕΠΙΚΕΦΑΛΙΔΑ ΠΙΣΤΟΠΟΙΗΣΗΣ

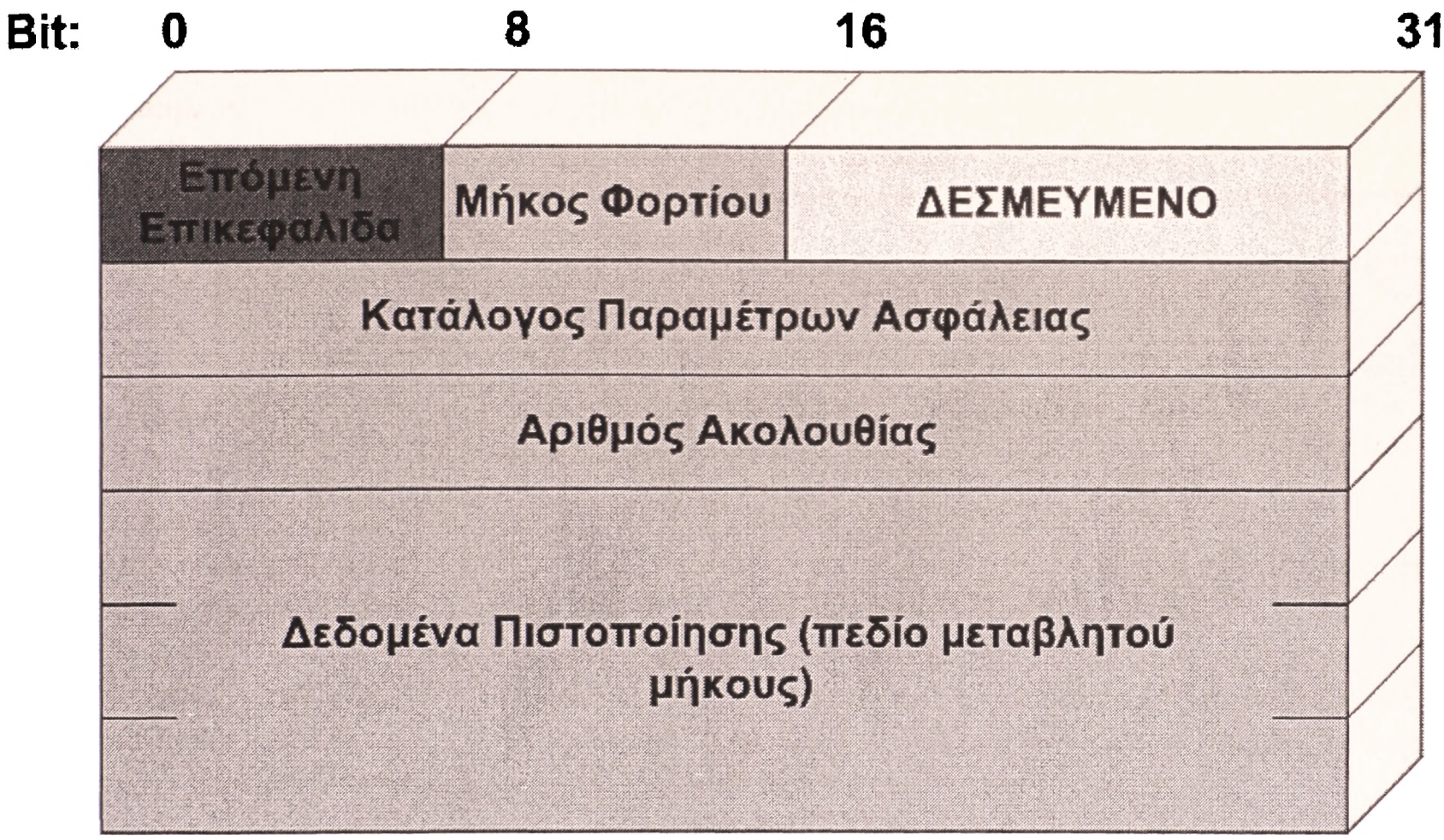
Η επικεφαλίδα πιστοποίησης παρέχει υποστήριξη για ακεραιότητα δεδομένων και πιστοποίηση των πακέτων IP. Το χαρακτηριστικό ακεραιότητας δεδομένων εξασφαλίζει πως είναι αδύνατο να μην ανιχνευθεί τροποποίηση στο περιεχόμενο ενός πακέτου κατά τη μεταφορά. Το χαρακτηριστικό πιστοποίησης επιτρέπει σε ένα τερματικό σύστημα ή μία συσκευή δικτύου να πιστοποιεί το χρήστη ή την εφαρμογή και να φιλτράρει ανάλογα την κίνηση. Επίσης εμποδίζει τις επιθέσεις εξαπάτησης διευθύνσεων που παρατηρούνται στο σημερινό Διαδίκτυο. Η πιστοποίηση βασίζεται στη χρήση ενός κώδικα πιστοποίησης μηνύματος (Message Authentication Code-MAC), για το λόγο αυτό οι δύο ομάδες πρέπει να διαμοιράζονται ένα μυστικό κλειδί.

Η επικεφαλίδα πιστοποίησης αποτελείται από τα ακόλουθα πεδία (Σχήμα 7-5):

- **Επόμενη Επικεφαλίδα - Next Header (8 bit):** Προσδιορίζει τον τύπο της επικεφαλίδας που ακολουθεί άμεσα αυτήν την επικεφαλίδα.
- **Μήκος Φορτίου - Payload Length (8 bit):** Το μήκος της επικεφαλίδας πιστοποίησης σε 32-bit λέξεις, μείον 2. Για παράδειγμα, το προεπιλεγμένο μήκος του πεδίου δεδομένων πιστοποίησης είναι 96 bit ή τρεις 32-bit λέξεις. Με μία σταθερή

επικεφαλίδα των τριών λέξεων, υπάρχει ένα σύνολο από έξι λέξεις στην επικεφαλίδα και το πεδίο Μήκος Φορτίου έχει μία τιμή 4.

- **ΔΕΣΜΕΥΜΕΝΟ - RESERVED (16 bit):** Για μελλοντική χρήση.
- **Κατάλογος Παραμέτρων Ασφαλείας - Security Parameters Index (32 bit):** Προσδιορίζει μία σχέση ασφαλείας.
- **Αριθμός Ακολουθίας – Sequence Number (32 bit):** Μία μονοτονικά αυξανόμενη τιμή μετρητή.
- **Δεδομένα Πιστοποίησης – Authentication Data (μεταβλητό):** Ένα μεταβλητού μήκους πεδίο (πρέπει να είναι ένας ολοκληρωμένος αριθμός των 32-bit λέξεων) που περιέχει την τιμή ελέγχου ακεραιότητας (ICV), ή MAC, για αυτό το πακέτο.



Σχήμα 7-5: Επικεφαλίδα Πιστοποίησης IPSec

Το Πεδίο Πιστοποίησης Δεδομένων υπολογίζεται πάνω στα παρακάτω:

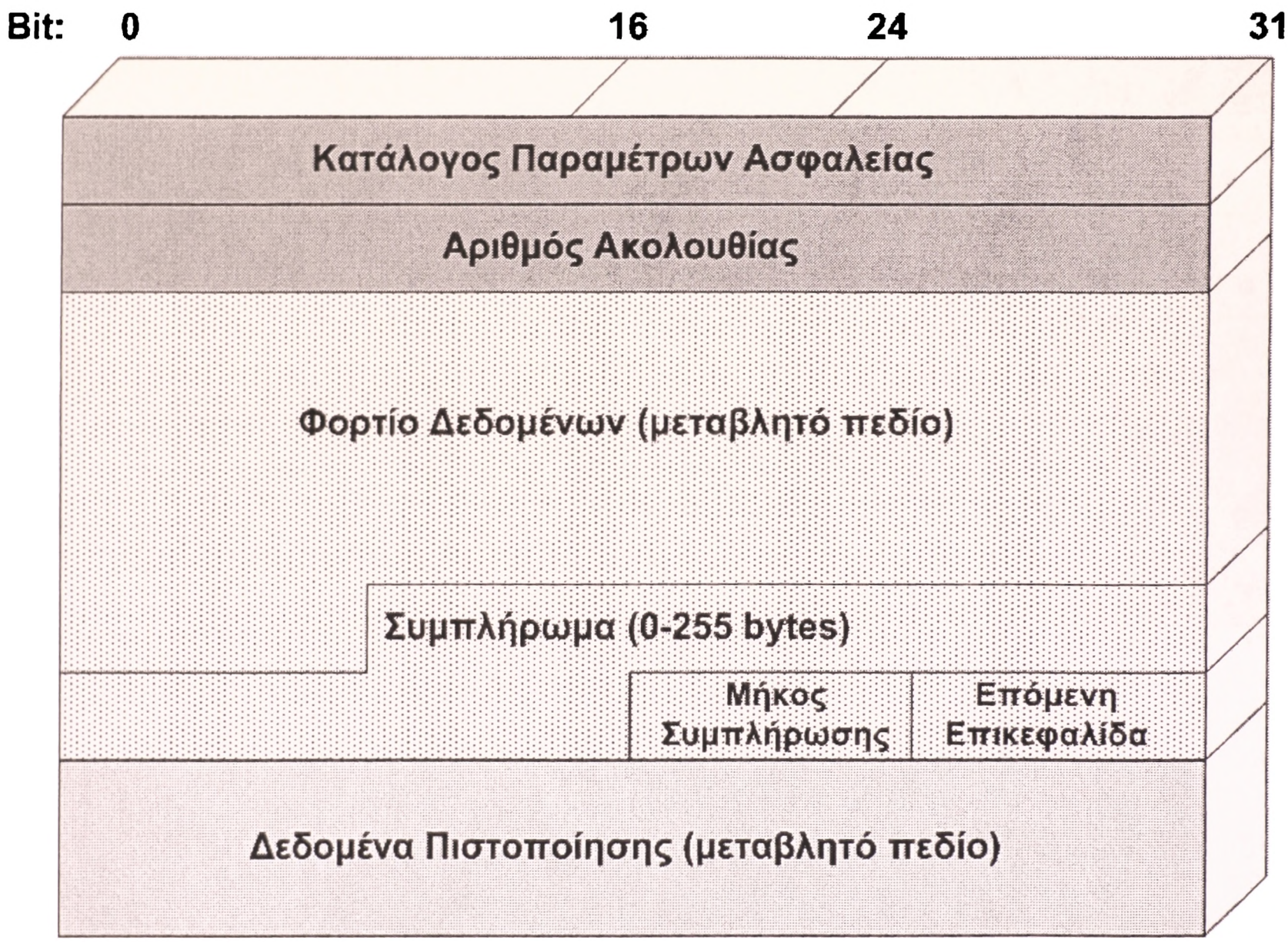
- Πεδία επικεφαλίδας IP που είτε δεν αλλάζουν στη μεταφορά (αμετάβλητα) είτε είναι προβλέψιμα στην τιμή επί της άφιξης στο ακραίο σημείο για την Επικεφαλίδα Πιστοποίησης.
  Πεδία που μπορεί να αλλάξουν στη μεταφορά και των οποίων η τιμή κατά την άφιξη είναι μη προβλέψιμη θέτονται στο μηδέν για λόγους υπολογισμού τόσο στην πηγή όσο και στον προορισμό.
- Την επικεφαλίδα AH αλλιώς το πεδίο Δεδομένων Πιστοποίησης. Το πεδίο Δεδομένων Πιστοποίησης τίθεται στο μηδέν για λόγους υπολογισμού τόσο στην πηγή όσο και στον προορισμό.

- Όλα τα δεδομένα πρωτοκόλλου ανωτέρου επιπέδου, τα οποία θεωρούνται αμετάβλητα κατά τη μεταφορά (π.χ., ένα τεμάχιο TCP ή ένα εσωτερικό πακέτο IP σε ρυθμό σήραγγας).

7.2.5 ΕΝΘΥΛΑΚΩΣΗ ΦΟΡΤΙΟΥ ΑΣΦΑΛΕΙΑΣ

Το ενθυλακωμένο φορτίο ασφαλείας παρέχει υπηρεσίες εμπιστευτικότητας, περιλαμβάνοντας εμπιστευτικότητα των περιεχομένων μηνύματος και εμπιστευτικότητα περιορισμένης ροής κίνησης. Ως προαιρετικό χαρακτηριστικό, το ESP μπορεί επίσης να παρέχει τις ίδιες υπηρεσίες πιστοποίησης με την AH.

Το παρακάτω σχήμα (σχήμα 7-6) παρουσιάζει τη μορφή ενός πακέτου ESP.



Σχήμα 7-6: Διάταξη του ESP IPSec

Το πακέτο ESP περιέχει τα ακόλουθα πεδία:

- **Κατάλογος παραμέτρων ασφαλείας – Security Parameters Index (32 bit):** Προσδιορίζει μία σχέση ασφάλειας.

- **Αριθμός ακολουθίας – Sequence Number (32 bit):** Μία μονοτονικά αυξανόμενη τιμή μετρητή.
- **Φορτίο δεδομένων (μεταβλητό) – Payload Data (variable):** Αυτό είναι ένα τεμάχιο επιπέδου μεταφοράς (τύπου μεταφοράς) ή πακέτο IP (τύπου σήραγγας) που προστατεύεται με κρυπτογράφηση.
- **Συμπλήρωμα - Padding (0 - 255 byte):** Μπορεί να απαιτείται εάν ο αλγόριθμος κρυπτογράφησης απαιτεί το μη κωδικοποιημένο κείμενο να είναι ένα πολλαπλάσιο κάποιου αριθμού από οκτάδες.
- **Μήκος συμπλήρωσης – Pad Length (8 bit):** Προσδιορίζει τον αριθμό των byte συμπλήρωσης αμέσως πριν αυτό το πεδίο.
- **Επόμενη επικεφαλίδα – Next Header (8 bit):** Προσδιορίζει τον τύπο των δεδομένων που περιέχονται στο πεδίο φορτίο δεδομένων προσδιορίζοντας την πρώτη επικεφαλίδα σε αυτό το φορτίο (για παράδειγμα, μία επικεφαλίδα επέκτασης στο IPv6 ή ένα πρωτόκολλο ανωτέρου επιπέδου όπως το TCP).
- **Δεδομένα πιστοποίησης (μεταβλητό) – Authentication Data (variable):** Ένα πεδίο μεταβλητού μήκους (πρέπει να είναι ένας ολοκληρωμένος αριθμός λέξεων των 32-bit) που περιέχει την τιμή ελέγχου ακεραιότητας που υπολογίστηκε επί του πακέτου ESP πλην του πεδίου δεδομένων πιστοποίησης.

7.2.6 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΟΥ

Το τμήμα διαχείρισης κλειδιού του IPSec περιλαμβάνει τον προσδιορισμό και την κατανομή των μυστικών κλειδιών. Το έγγραφο της Αρχιτεκτονικής του IPSec διευθύνει υποστήριξη για δύο τύπους διαχείρισης κλειδιού:

- **Χειροκίνητη:** Ένας διαχειριστής του συστήματος ρυθμίζει χειροκίνητα κάθε σύστημα με τα δικά του κλειδιά και με τα κλειδιά άλλων επικοινωνούντων συστημάτων. Αυτό είναι πρακτικό για μικρά, σχετικά στατικά συστήματα.
- **Αυτοματοποιημένη:** Ένα αυτοματοποιημένο σύστημα επιτρέπει την επί της ζήτησης δημιουργία κλειδιών για SAs και διευκολύνει τη χρήση των κλειδιών σε ένα μεγάλο κατανεμημένο σύστημα με μία αναπτυσσόμενη διάταξη. Ένα αυτοματοποιημένο σύστημα είναι το περισσότερο ευέλικτο αλλά απαιτεί περισσότερη προσπάθεια για να ρυθμιστεί και απαιτεί περισσότερο λογισμικό, οπότε μικρότερες εγκαταστάσεις είναι πιθανό να επιλέγουν υπέρ της χειροκίνητης διαχείρισης κλειδιού.

Το προεπιλεγμένο πρωτόκολλο αυτοματοποιημένης διαχείρισης κλειδιού για το IPSec αναφέρεται ως ISAKMP/Oakley, αποτελούμενο από τα ακόλουθα στοιχεία:

- **Πρωτόκολλο προσδιορισμού κλειδιού Oakley:** Το Oakley είναι ένα πρωτόκολλο ανταλλαγής κλειδιού βασισμένο στον αλγόριθμο Diffie-Hellman [Diff76], αλλά παρέχει επιπρόσθετη ασφάλεια. Συγκεκριμένα ο Diffie-Hellman δεν πιστοποιεί από μόνος του τους δύο χρήστες που ανταλλάσσουν κλειδιά, κάνοντας το πρωτόκολλο ευπρόσβλητο στην προσωποποίηση. Το Oakley περιλαμβάνει μηχανισμούς για να πιστοποιεί τους χρήστες.

- **Πρωτόκολλο Σχέσης Ασφαλείας Διαδικτύου και Διαχείρισης Κλειδιού (ISAKMP):** Το ISAKMP παρέχει ένα πλαίσιο εργασίας για διαχείριση κλειδιού Διαδικτύου και παρέχει την ειδική υποστήριξη πρωτοκόλλου, περιλαμβάνοντας τις διατάξεις, για διαπραγμάτευση των χαρακτηριστικών ασφαλείας.

Το ISAKMP από μόνο του δεν υπαγορεύει ένα συγκεκριμένο μηχανισμό διαχείρισης κλειδιού. Αντίθετα, το ISAKMP αποτελείται από ένα σύνολο από τύπους μηνυμάτων που επιτρέπουν τη χρήση μίας ποικιλίας από αλγορίθμους ανταλλαγής κλειδιού. Το Oakley είναι ο συγκεκριμένος αλγόριθμος ανταλλαγής κλειδιού που καθορίζεται για χρήση με την αρχική έκδοση του ISAKMP.

7.2.7 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ IPSec

Οι πολιτικές ασφάλειας μέσα από το πλαίσιο του IPSec επιτρέπουν στους διαχειριστές δικτύων να ελέγξουν τον τρόπο με τον οποίο η εισερχόμενη και εξερχόμενη δικτυακή κυκλοφορία υποβάλλεται σε επεξεργασία καθώς περνά μέσα από τις υπηρεσίες ασφάλειας του IPSec [Kent 98]. Όταν τα εισερχόμενα πακέτα παραδίδονται στη μηχανή επεξεργασίας του IPSec από το δίκτυο, αυτά «τρέχουν» μέσα από μια διαδικασία η οποία καθορίζει ποιες ενέργειες πρέπει να γίνουν πάνω στα πακέτα αυτά. Οι ενέργειες αυτές βασίζονται στην πολιτική ασφάλειας του εγκατεστημένου συστήματος.

Οι πολιτικές που ορίζει το IPSec ισχύουν τόσο για τα εισερχόμενα όσο και για τα εξερχόμενα πακέτα δεδομένων τα οποία «ταξιδεύουν» προς η διαμέσου μιας δικτυακής συσκευής. Λειτουργικά, οι βάσεις δεδομένων της πολιτικής ασφάλειας του IPSec σχεδιάζονται για να απαντήσουν τις ακόλουθες βασικές ερωτήσεις:

- **Με ποιους επιτρέπεται να εκτελούνται συναλλαγές;**
- **Ποιοι παράμετροι πρέπει να επιβληθούν πάνω σε αυτές τις συναλλαγές;**
- **Τι θα πρέπει να γίνει με τα πακέτα που δεν καλύπτουν αυτές τις απαιτήσεις;**

Η βάση δεδομένων της σχέσης ασφάλειας (Security Association Database – SAD) του IPSec περιέχει πληροφορίες σχετικά με τις ισχύουσες συνδέσεις που χρησιμοποιούνται μέσα από μια δεδομένη συσκευή, η οποία ερωτάται πότε πρέπει να εφαρμοστούν οι υπηρεσίες πιστοποίησης και κρυπτογράφησης/αποκρυπτογράφησης, τόσο για τα εισερχόμενα όσο και για τα εξερχόμενα πακέτα. Οι πολιτικές ασφάλειας του IPSec που επηρεάζουν αυτή τη βάση δεδομένων (SAD), υπαγορεύουν τι θα συμβεί όταν τα πακέτα αυτά δεν ταιριάζουν κατάλληλα στις απαιτήσεις της βάσης δεδομένων (SAD).

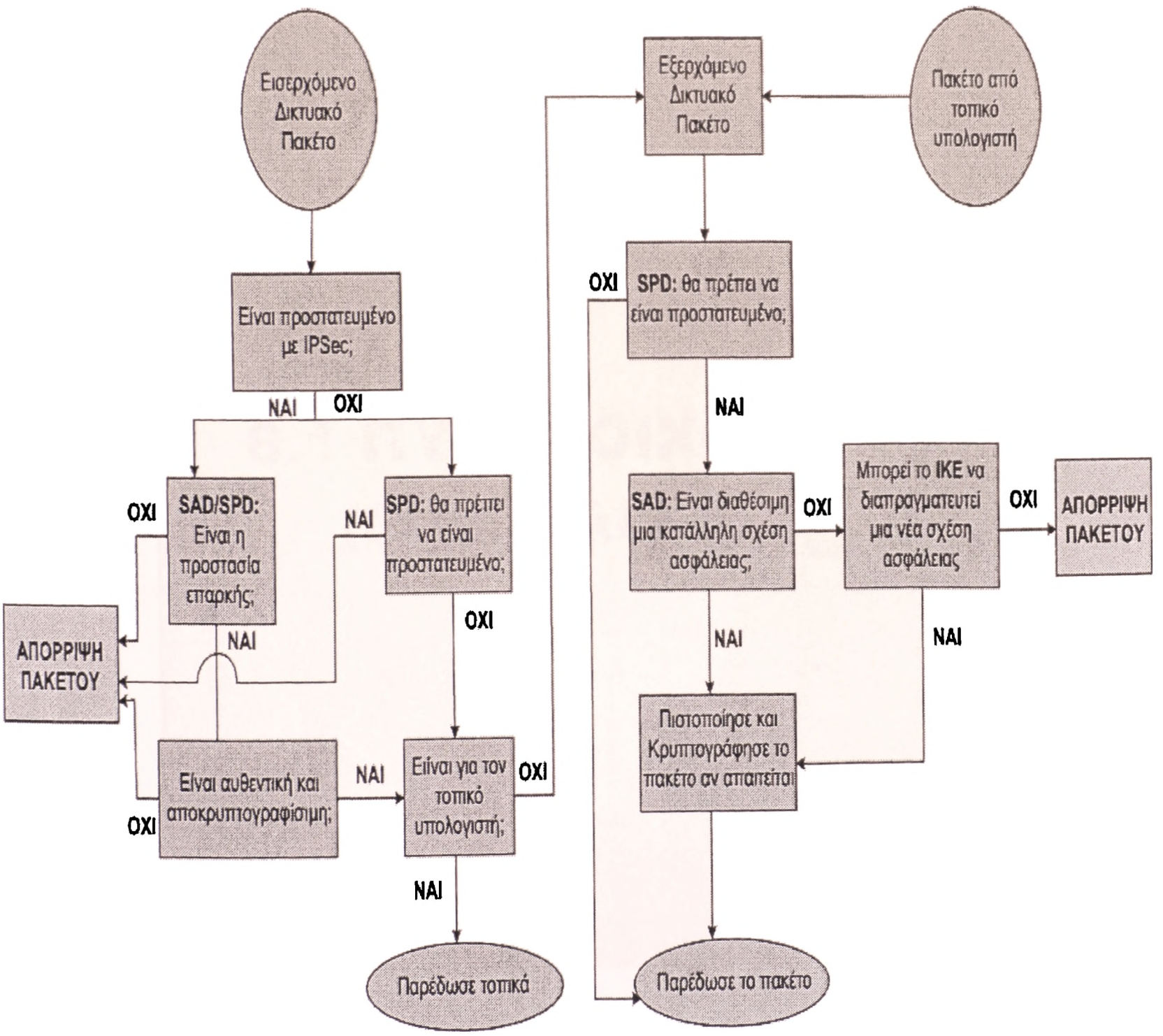
Η βάση δεδομένων της πολιτικής ασφάλειας (Security Policy Database – SPD) ελέγχει συνολικά τις απαιτήσεις επεξεργασίας του IPSec από μια συσκευή. Η βάση δεδομένων της πολιτικής ασφάλειας καθορίζει εάν η δικτυακή κυκλοφορία δεδομένων μεταξύ δυο οντοτήτων θα πρέπει να ελέγχεται από το IPSec ή επιτρέπεται να περάσει απροστάτευτη. Αυτή η βάση δεδομένων λειτουργεί ως ένας μηχανισμός διαμόρφωσης, η οποία «κάθεται» πάνω στη βάση δεδομένων SAD. Η βάση δεδομένων της πολιτικής ασφάλειας (SPD) διαμορφώνει την βάση δεδομένων της σχέσης ασφάλειας (SAD), έτσι ώστε αυτή (SAD) να εφαρμόσει την πολιτική ασφάλειας η οποία έχει καθοριστεί από τον διαχειριστή ασφάλειας.

Εάν ένα εισερχόμενο δικτυακό πακέτο δεν προστατεύεται από το IPSec τότε η βάση δεδομένων της πολιτικής ασφάλειας (SPD) ερωτάται για να αποφασίσει τι θα πρέπει να κάνει

με το πακέτο αυτό. Η απόφαση που θα πάρει η βάση δεδομένων της πολιτικής ασφάλειας βασίζεται τόσο στην πηγή από την οποία προήλθε το πακέτο όσο και τον προορισμό τον οποίο έχει το πακέτο αυτό. Η ενέργεια που θα γίνει μπορεί να περιλαμβάνει: απόρριψη του πακέτου, έναρξη μιας νέας ικανής IPSec σύνδεσης, χρησιμοποίηση μιας ήδη υπάρχουσας σύνδεσης IPSec ή αναγραφή ενός λάθους ή μιας προειδοποίησης.

Το πρωτόκολλο Ανταλλαγής Κλειδιών Διαδικτύου (Internet Key Exchange – IKE) περιγράφει ορισμένες επιπρόσθετες πολιτικές ασφάλειας οι οποίες θα πρέπει να επιβληθούν κατά τη διαδικασία διαπραγμάτευσης των κλειδιών, όταν δημιουργούνται σχέσεις ασφάλειας IPSec. Οι πολιτικές που μπορούν να εφαρμόζονται στο πρωτόκολλο Ανταλλαγής Κλειδιών Διαδικτύου περιλαμβάνουν το πόσο συχνά τα κλειδιά θα πρέπει να ενημερώνονται (updated), πότε απαιτείται τέλεια μυστικότητα κατά τη διάρκεια της ανταλλαγής των κλειδιών κ.λ.π.

Ένα δέντρο απόφασης το οποίο απεικονίζει απλοποιημένη εκδοχή αυτής της επεξεργασίας φαίνεται στο παρακάτω σχήμα (σχήμα 7-7).



Σχήμα 7-7: Πολιτική Δέντρου Απόφασης (Decision Tree) του IPSec

ΚΕΦΑΛΑΙΟ 8ο

8.1 ΠΥΡΟΤΟΙΧΟΙ (FIREWALLS)

8.1 ΠΥΡΟΤΟΙΧΟΙ (FIREWALLS)

Όταν ένα ιδιόκτητο δίκτυο συνδέεται σε ένα δημόσιο, οι χρήστες του μπορούν να έχουν πρόσβαση και να επικοινωνούν με αυτό. Ταυτόχρονα, όμως, και οι χρήστες του δημοσίου δικτύου μπορούν να επικοινωνήσουν με το ιδιόκτητο δίκτυο, γεγονός που δημιουργεί σημαντικά προβλήματα ασφάλειας. Λύση στο πρόβλημα αυτό μπορεί να αποτελέσει ένα ενδιάμεσο σύστημα που θα παρεμβληθεί μεταξύ του ιδιόκτητου και του δημόσιου δικτύου, θα αποτελεί σημείο ελέγχου και θα υλοποιεί ένα τείχος ασφάλειας. Σκοπός αυτού του ενδιάμεσου συστήματος είναι να προστατεύει το ιδιόκτητο δίκτυο από επιθέσεις που προέρχονται από τον έξω κόσμο και να παρέχει ένα μοναδικό σημείο ελέγχου, όπου μπορεί να ελεγχθεί η κίνηση από και προς αυτό το δίκτυο. Επίσης, το σύστημα αυτό μπορεί να χρησιμοποιηθεί και για συλλογή πληροφοριών διαχείρισης για τη χρήση του δικτύου. Ως μοναδικό σημείο διέλευσης των πακέτων, το ενδιάμεσο αυτό σύστημα μπορεί να καταγράφει οτιδήποτε διακινείται μεταξύ του τοπικού δικτύου και του έξω κόσμου. Τέτοια ενδιάμεσα συστήματα ονομάζονται «πυρότοιχοι». Ουσιαστικά, ένας πυρότοιχος είναι ένας «τοίχος» ασφάλειας μεταξύ ενός ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο και ενός δημόσιου, όπως το Διαδίκτυο, το οποίο θεωρείται μη ασφαλές. Σκοπός ενός πυρότοιχου είναι να εμποδίσει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία από και προς αυτό το δίκτυο.

Η χρήση ενός πυρότοιχου δεν αποτελεί πανάκεια για την ασφάλεια του δικτύου. Όπως και οποιοδήποτε σύστημα ασφάλειας μπορεί κι αυτό να παραβιαστεί αν κάποιος ικανός εισβολέας καταβάλλει αρκετή προσπάθεια. Ωστόσο, αυτό που επιτυγχάνεται με ένα καλό πυρότοιχο είναι να καταστεί η προσπάθεια για την παραβίαση του τόσο μεγάλη, ώστε ο εισβολέας να διαλέξει κάποιον πιο εύκολο στόχο. Σε περίπτωση πάντως που ο εισβολέας παραβιάσει την ασφάλεια και μπει στο δίκτυο, θα πρέπει να χρησιμοποιηθούν επιπλέον συστήματα για την προστασία των πολύτιμων δεδομένων.

8.1.1 ΟΡΙΣΜΟΣ ΤΩΝ ΠΥΡΟΤΟΙΧΩΝ

Πυρότοιχος ονομάζεται ένα σύστημα που αποτελείται από δικτυακά στοιχεία τα οποία τοποθετούνται μεταξύ δύο δικτύων και το οποίο έχει τα ακόλουθα χαρακτηριστικά:

1) Όλη η δικτυακή κίνηση από και προς το εσωτερικό δίκτυο πρέπει να περάσει μέσα από αυτό το σύστημα.
2) Η διέλευση επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες, όπως αυτή καθορίζεται από την τοπική πολιτική ασφάλειας.
3) Είναι αδιαπέραστο σε απόπειρες διείσδυσης.

Ο όρος πυρότοιχος αναφέρεται σε οποιοδήποτε συνδυασμό στοιχείων υλικού, λογισμικού και πολιτικής ασφάλειας που τοποθετείται μεταξύ ενός ιδιωτικού (συνήθως ένα ενδοεπιχειρησιακό δίκτυο) και ενός εξωτερικού δικτύου (συνήθως το Διαδίκτυο). Ως τέτοιος, ο πυρότοιχος υλοποιεί κάποια μέρη της λεγόμενης **Πολιτικής Ασφαλείας Δικτύου** (**NSP-Network Security Policy**) με το να αναγκάζει όλη την κίνηση δεδομένων να κατευθυνθεί ή να δρομολογηθεί προς αυτό, όπου μπορεί να εξεταστεί και να αποφασιστεί αν θα επιτραπεί η

διέλευση της. Δηλαδή, ο πυρότοιχος προσπαθεί να αποτρέψει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία από και προς το ενδοεπιχειρησιακό δίκτυο (intranet) καθώς και να επιτρέψει στον οργανισμό να επιβάλει μια πολιτική ασφάλειας σχετικά με τη ροή των δεδομένων μεταξύ του ιδιόκτητου δικτύου και του Διαδικτύου. Ένα τυπικό σύστημα με πυρότοιχο μπορεί να επιτρέπει επιλεκτικά την πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και κωδικούς πρόσβασης ή σε IP διευθύνσεις ή ακόμη και σε ονόματα πεδίων (domain names). Ένας πυρότοιχος μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει την κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής ελέγχου (control policy) που υποστηρίζει και εξαρτάται από τη συγκεκριμένη διαμόρφωση του (configuration). Ως ένα σύστημα πυρότοιχου μπορεί να θεωρηθεί μια διάταξη δρομολόγησης (router), ένας προσωπικός υπολογιστής, ένας διακομιστής ή ένα σύνολο από διακομιστές διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία ή ένα υποδίκτυο από πρωτόκολλα και υπηρεσίες (FTP, HTTP, e-mail, κλπ.).

8.1.2 ΒΑΣΙΚΕΣ ΤΕΧΝΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ

Οι βασικές τεχνικές προστασίας είναι οι τρεις παρακάτω:

1) Πύλες φιλτραρίσματος πακέτων (packet filtering gateways) ή δρομολογητές φιλτραρίσματος (screening routers)
2) Πύλες κυκλωμάτων (circuit gateways)
3) Πύλες εφαρμογών (application gateways)

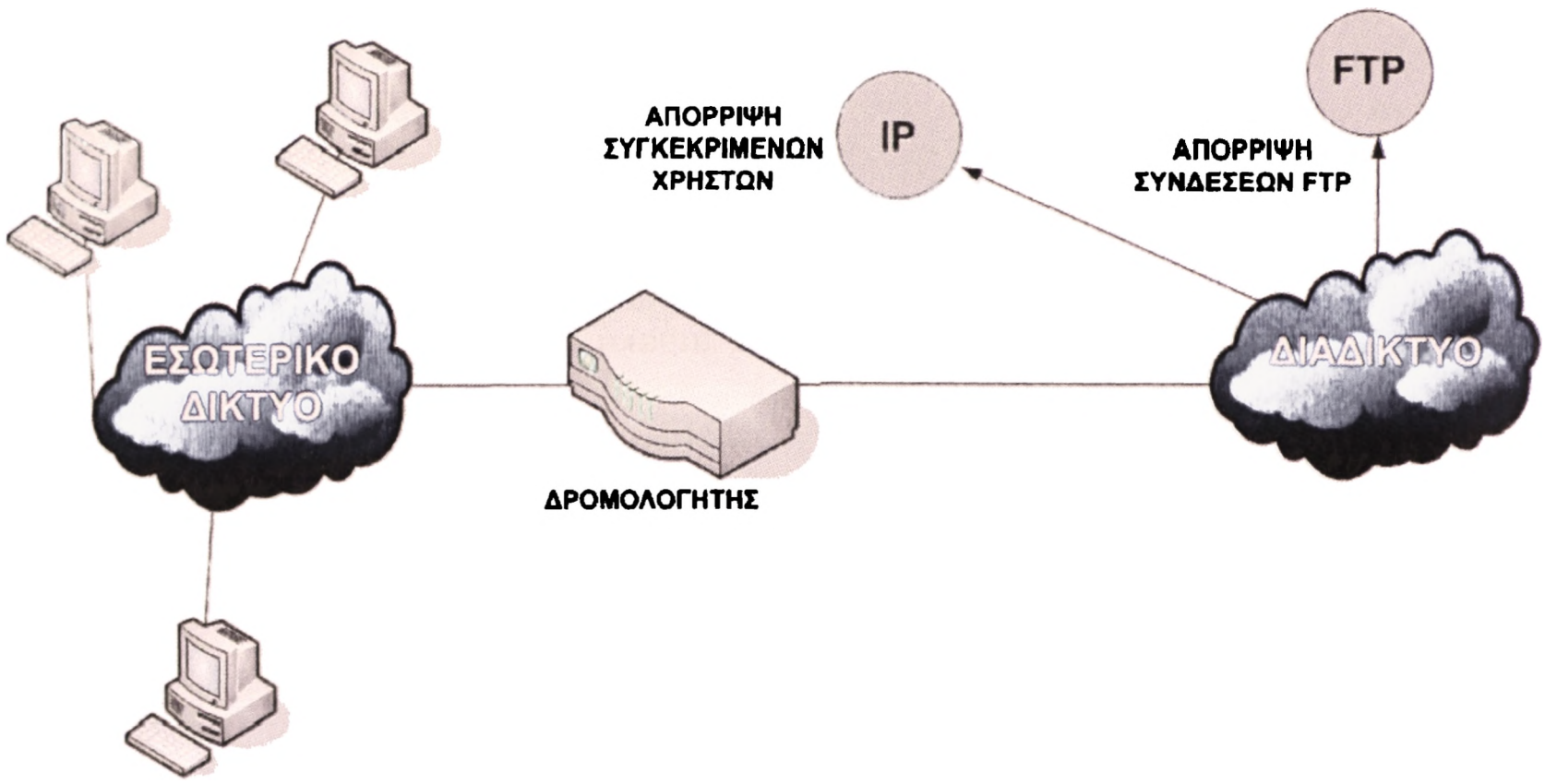
Μια ολοκληρωμένη υπηρεσία πυρότοιχων συνήθως παρέχεται με συνδυασμό των παραπάνω τεχνικών φιλτραρίσματος.

8.1.2.1 ΔΡΟΜΟΛΟΓΗΤΕΣ ΦΙΛΤΡΑΡΙΣΜΑΤΟΣ (SCREENING ROUTERS)

Αυτή η τεχνική είναι η πρώτη που εμφανίστηκε ως συνοδευτικό εργαλείο λογισμικού για την υποστήριξη επιπλέον ρυθμίσεων στον αρχικά απλό εξοπλισμό των διατάξεων ή συσκευών δρομολόγησης που είχαν δυνατότητα φιλτραρίσματος πακέτων. Το φίλτρο πακέτων διενεργεί τον έλεγχο εφαρμόζοντας ένα σύνολο κανόνων οι οποίοι έχουν οριστεί από το διαχειριστή του πυρότοιχου κατά τη διαμόρφωση του και οι οποίοι υλοποιούν μια προαποφασισμένη πολιτική ασφάλειας. Η υλοποίηση της τεχνικής αυτής μπορεί να γίνει είτε πάνω σε ένα συγκεκριμένο υπολογιστή είτε σε κάποια ηλεκτρονική συσκευή με ικανότητες δρομολόγησης που μπορεί να προγραμματιστεί απομακρυσμένα. Ο προγραμματισμός των κριτηρίων γίνεται με κάποιο ειδικό λογισμικό για δρομολογητές (routers) ή διακόπτες (switches). Αφού ολοκληρωθεί ο προγραμματισμός του τοποθετείται ακριβώς στο σημείο επαφής του εσωτερικού δικτύου με τα άλλα εξωτερικά δίκτυα. Τα κριτήρια επιλογής των πακέτων για τα οποία επιτρέπεται ή όχι η είσοδος στο εσωτερικό δίκτυο, βασίζονται στις ακόλουθες παραμέτρους:

- Διεύθυνση προέλευσης και προορισμού: για τις IP διευθύνσεις μπορούν να χρησιμοποιηθούν και μάσκες διευθύνσεων που ομαδοποιούν τις διευθύνσεις.
- Αριθμός θύρας προέλευσης και προορισμού: σε κάθε διακομιστή οι εκτελούμενες εφαρμογές καταλαμβάνουν συγκεκριμένους αριθμούς θυρών επικοινωνίας (ports).
- Πρωτόκολλο: π.χ. TCP-Transfer Control Protocol, UDP-User Datagram Protocol.
- Κατεύθυνση: ανάλογα με το αν εισέρχεται το πακέτο στο εσωτερικό δίκτυο ή εξέρχεται από αυτό.

Στο Σχήμα 8-1 φαίνεται μια διάταξη ενός πυρότοιχου (firewall) με βάση την τεχνολογία ενός δρομολογητή φιλτραρίσματος που απορρίπτει συγκεκριμένες IP διευθύνσεις και αιτήσεις για συνδέσεις με βάση το πρωτόκολλο μεταφοράς αρχείου (File Transfer Protocol-FTP).



Σχήμα 8-1: Διάταξη πυρότοιχου με τεχνολογία δρομολογητή φιλτραρίσματος απορρίπτει εισερχόμενες FTP συνδέσεις και συγκεκριμένες IP διευθύνσεις

Από την άλλη η τεχνική αυτή παρουσιάζει και αρκετούς περιορισμούς, όπως:

- Ο έλεγχος που πραγματοποιείται αφορά κυρίως το είδος της κυκλοφορίας του δικτύου, αφού εξετάζονται μόνο οι IP επικεφαλίδες κάθε πακέτου και όχι το περιεχόμενο του πακέτου. Στην επικεφαλίδα υπάρχουν οι απαραίτητες πληροφορίες δρομολόγησης (προέλευση και προορισμός του πακέτου). Επειδή όμως το περιεχόμενο δεν εξετάζεται η τεχνική αυτή είναι κατάλληλη για απλές σχετικά πολιτικές ασφάλειας.
- Δεν προσφέρει επαρκείς μηχανισμούς επίβλεψης και ειδοποίησης κινδύνου
- Δεν υποστηρίζει εύκολη διαχείριση γιατί υπάρχει περιορισμένος αριθμός κανόνων οι οποίοι μάλιστα απαιτούν κατανόηση των ιδιαιτεροτήτων των πρωτοκόλλων επικοινωνίας. Έτσι είναι αρκετά σύνθετο και δύσκολο έργο η ορθή διαμόρφωση τους για την εφαρμογή μιας πολιτικής ασφάλειας. Βέβαια διατίθενται κάποια

εργαλεία υποστήριξης του έργου των διαχειριστών που ελέγχουν τη σύνταξη κανόνων, κάνουν λιγότερο άβολο το περιβάλλον διεπαφής (user interface), κλπ.

- Δεν προσφέρει επαρκείς μηχανισμούς επίβλεψης και ειδοποίησης κινδύνου
- Δεν υποστηρίζει εύκολη διαχείριση γιατί υπάρχει περιορισμένος αριθμός κανόνων οι οποίοι μάλιστα απαιτούν κατανόηση των ιδιαιτεροτήτων των πρωτοκόλλων επικοινωνίας. Έτσι είναι αρκετά σύνθετο και δύσκολο έργο η ορθή διαμόρφωση τους για την εφαρμογή μιας πολιτικής ασφάλειας. Βέβαια διατίθενται κάποια εργαλεία υποστήριξης του έργου των διαχειριστών που ελέγχουν τη σύνταξη κανόνων, κάνουν λιγότερο άβολο το περιβάλλον διεπαφής (user interface), κλπ.
- Δεν διαθέτουν συνήθως μηχανισμούς αυθεντικοποίησης σε επίπεδο χρήστη
- Δεν προστατεύουν από επιθέσεις πλαστογράφησης της IP διεύθυνσης (IP Spoofing) . Η βασική αδυναμία της τεχνικής αυτής είναι ότι στηρίζεται στις IP διευθύνσεις, οι οποίες όμως δεν είναι απόλυτα ασφαλείς και δεν προστατεύονται.

8.1.2.2 ΠΥΛΕΣ ΚΥΚΛΩΜΑΤΩΝ (CIRCUIT GATEWAYS)

Η χρήση των πυλών κυκλωμάτων σε διατάξεις πυρότοιχων (firewalls) αναβαθμίζει σημαντικά την ασφάλεια των δικτύων. Επιτρέπουν τη χρήση εφαρμογών που βασίζονται στα πρωτόκολλα επικοινωνίας TCP και UDP (όπως για παράδειγμα WWW, telnet, κλπ) χωρίς να αφήνουν να γίνονται όλα σε επίπεδο πρωτοκόλλου επικοινωνίας. Οι πύλες κυκλωμάτων λειτουργούν ως πληρεξούσιοι (proxies) των πρωτοκόλλων επικοινωνίας, μεταβιβάζοντας την κίνηση μεταξύ δύο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους μέσω ενός ιδεατού κυκλώματος (virtual circuit). Ο πυρότοιχος (firewall) μπορεί να χρησιμοποιηθεί ώστε να καταγραφεί και την ποσότητα των μεταβιβαζόμενων δεδομένων και του προορισμού τους. Επίσης, μπορεί να ελέγξει το περιεχόμενο των δεδομένων. Τέλος, η ύπαρξη ενός εκπροσώπου (proxy) για όλες τις υπηρεσίες κάνει εύκολη τη διαχείριση του συστήματος του πυρότοιχου σε σχέση με τις τεχνικές των πυλών των εφαρμογών, ενώ παρέχουν ασφάλεια για ένα μεγάλο σύνολο υπηρεσιών.

8.1.2.3 ΠΥΛΕΣ ΕΦΑΡΜΟΓΩΝ (APPLICATION GATEWAYS)

Η τεχνική αυτή είναι παρόμοια με αυτή των πυλών κυκλωμάτων με τη διαφορά ότι για κάθε εφαρμογή που υποστηρίζεται υπάρχει και ο αντίστοιχος πληρεξούσιος εξυπηρετητής που ελέγχει την κυκλοφορία. Η τεχνική αυτή λειτουργεί στο υψηλότερο επίπεδο επικοινωνίας (application layer). Έτσι τα συστήματα πυρότοιχου με αυτή την τεχνική αποκτούν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα κάνοντας τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας. Όλα τα IP (Internet Protocol) πακέτα που φτάνουν εξετάζονται πρώτα ως προς το περιεχόμενο τους και ανάλογα προωθούνται ή απορρίπτονται. Ο έλεγχος αυτός γίνεται από τον αντίστοιχο εκπρόσωπο (proxy). Για παράδειγμα, ένας χρήστης προερχόμενος από το Διαδίκτυο, για να αποκτήσει πρόσβαση στην υπηρεσία του πρωτοκόλλου μεταφοράς αρχείων (File Transfer Protocol – FTP) ενός υπολογιστή που προστατεύεται με βάση αυτή την τεχνική, θα πρέπει πρώτα να συνδεθεί με την αντίστοιχη proxy εφαρμογή, να ακολουθήσει η διαδικασία ταυτοποίησης και

πιστοποίησης του, και αφού η σύνδεση εγκριθεί θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε.

8.1.2.4 ΥΒΡΙΔΥΚΕΣ ΠΥΛΕΣ

Είναι γενική αίσθηση ότι για ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών επιπέδου πακέτων και επιπέδου εφαρμογής. Έτσι παρατηρείται μια τάση σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστημάτων πυρότοιχων για περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας. Ο όρος υβριδικές ή σύνθετες πύλες χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα πυρότοιχων που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών, προχωρούν ένα βήμα πιο πέρα. Ένα παράδειγμα είναι ο συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών.

Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών

Ο έλεγχος αποκλειστικά των IP κεφαλίδων είναι μια λειτουργία που κάθε πυρότοιχος χρειάζεται, γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου. Έτσι ακόμα και οι καθαρά proxy πυρότοιχοι διαθέτουν λογισμικό που προσομοιώνει έναν δρομολογητή φιλτραρίσματος. Επειδή όμως αυξάνει κατά πολύ η ασφάλεια ενός συστήματος όταν δεν είναι συγκεντρωμένη η άμυνα του σε ένα μοναδικό σημείο, πολλές φορές ένα proxy-based σύστημα πυρότοιχου συνδυάζεται με μια επιπλέον διάταξη φίλτρου πακέτων. Η σύνδεση τους πρέπει να γίνει φυσικά σε σειρά έτσι ώστε οι επικοινωνίες να διέρχονται και από τα δύο αυτά συστατικά μέρη.

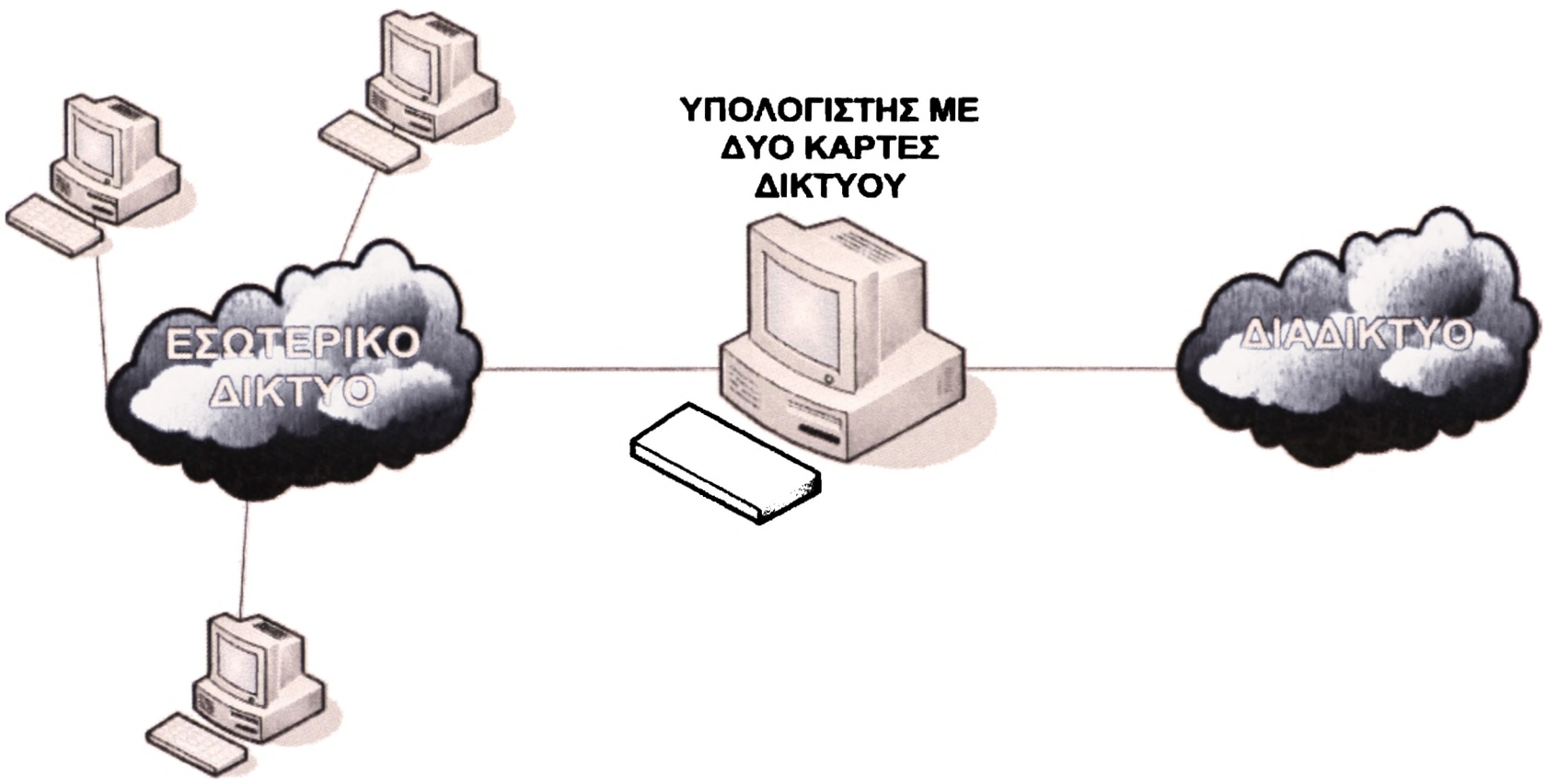
8.1.3 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΣΥΣΤΗΜΑΤΩΝ ΠΥΡΟΤΟΙΧΩΝ

Ένα ολοκληρωμένο σύστημα πυρότοιχου μπορεί να αποτελείται από πολλά συστατικά, χωρίς να είναι και όλα απαραίτητα. Τα διαφορετικά μέρη που μπορεί να διακρίνει κανείς στη σχεδίαση ενός τέτοιου συστήματος είναι τα παρακάτω:

- Μηχανισμός φίλτρου πακέτου: για να εμποδίζεται η πορεία των διακινούμενων πακέτων δεδομένων ανάμεσα στο Διαδίκτυο και το ιδιωτικό δίκτυο και να επιτρέπεται η κίνηση τους μέσω του πυρότοιχου μόνο σε όσα πακέτα ανήκουν σε αποδεκτούς τρόπους επικοινωνίας.
- Λογισμικό υλοποίησης πυλών σε επίπεδο εφαρμογής: ικανό να εμποδίζει την κυκλοφορία των δεδομένων και να πιστοποιεί τους χρήστες σε επίπεδο εφαρμογών TCP/IP.
- Υπηρεσία Ονομασίας Πεδίων (Domain Name Service - DNS): ικανή για την απόκρυψη των εσωτερικών IP διευθύνσεων του ιδιωτικού δικτύου από τους χρήστες του Διαδικτύου.
- Μηχανισμός διαχείρισης ηλεκτρονικών γραμμάτων: για να διασφαλίζεται ότι η ανταλλαγή ηλεκτρονικών γραμμάτων διεκπεραιώνεται μέσω πυρότοιχου.
- Ασφαλές λειτουργικό σύστημα: σαν βάση του όλου συστήματος.

8.1.3.1 ΥΠΟΛΟΓΙΣΤΗΣ ΜΕ ΔΙΠΛΗ ΚΑΡΤΑ ΔΙΚΤΥΟΥ (DUAL-HOMED HOST)

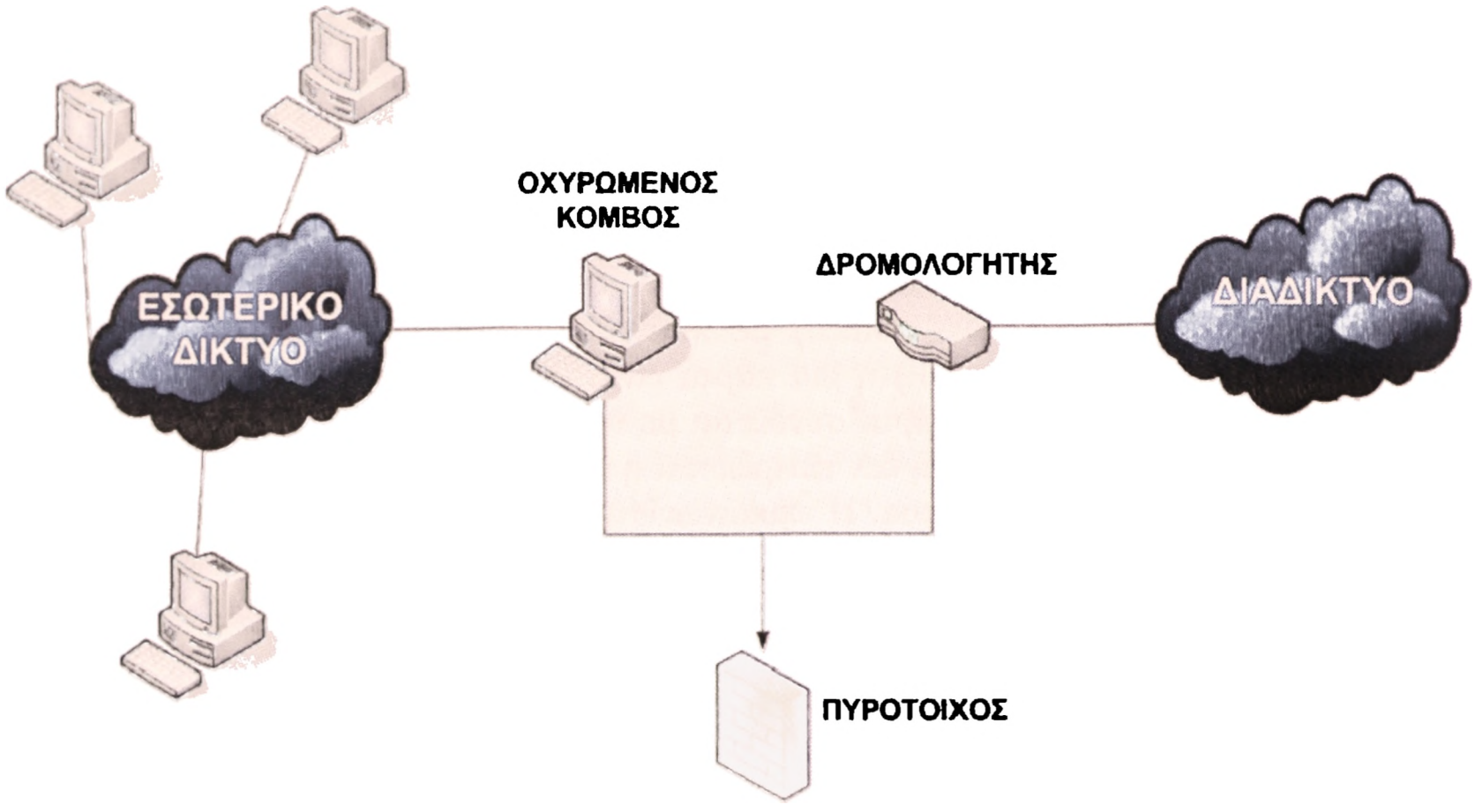
Στην αρχιτεκτονική αυτή χρησιμοποιείται σαν κεντρικός υπολογιστής ένας διακομιστής που διαθέτει περισσότερες από μία κάρτες δικτύου. Κάθε κάρτα είναι συνδεδεμένη σε ένα τμήμα δικτύου που είναι λογικά και φυσικά διαχωρισμένο. Η πιο διαδεδομένη μορφή της είναι με δύο κάρτες δικτύου (dual-homed). Σε ένα πυρότοιχο με υπολογιστή με διπλή κάρτα δικτύου (dual-homed host firewall) η μία κάρτα είναι συνδεδεμένη στο εξωτερικό και μη έμπιστο διαδίκτυο, ενώ η άλλη κάρτα συνδέεται με το εσωτερικό και θεωρούμενο ασφαλές δίκτυο. Σε αυτή την αρχιτεκτονική δεν επιτρέπεται η άμεση δρομολόγηση των πακέτων των δεδομένων ανάμεσα στα δύο δίκτυα. Η επικοινωνία τους πρέπει να γίνεται μόνο μέσω του λογισμικού του πυρότοιχου του διακομιστή. Στο παρακάτω σχήμα (σχήμα 8-2) φαίνεται ένα σύστημα πυρότοιχου με έναν υπολογιστή με δυο κάρτες δικτύου.



Σχήμα 8-2: Πυρότοιχος με υπολογιστή με δυο κάρτες δικτύου

8.1.3.2 ΠΥΡΟΤΟΙΧΟΙ ΥΠΟΛΟΓΙΣΤΗ ΔΙΑΛΟΓΗΣ (SCREENED HOST)

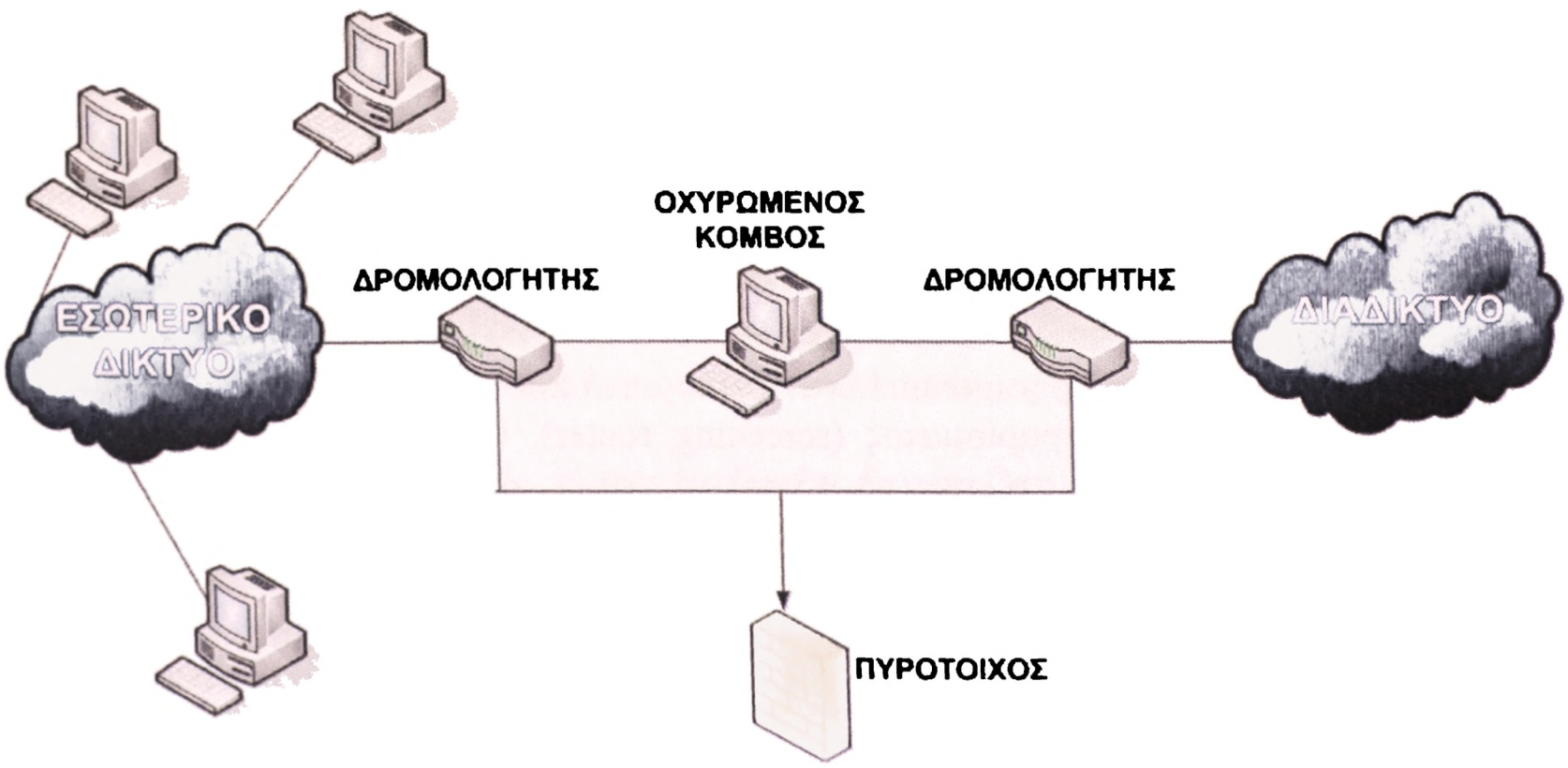
Αυτή η αρχιτεκτονική χρησιμοποιεί έναν διακομιστή που καλείται οχυρό (bastion host) και έναν δρομολογητή φιλτραρίσματος (screening router). Ο δρομολογητής αυτός είναι διαμορφωμένος ώστε να στέλνει αποκλειστικά στον οχυρωμένο κόμβο όλες τις προερχόμενες από το εξωτερικό δίκτυο αιτήσεις, όποιον προορισμό και να είχαν αυτές μέσα στο εσωτερικό δίκτυο. Όλοι λοιπόν οι εξωτερικοί διακομιστές υποχρεωτικά περνούν μέσω του λογισμικού πυρότοιχου στον οχυρωμένο κόμβο. Στο παρακάτω σχήμα (σχήμα 8-3) απεικονίζεται ένα σύστημα πυρότοιχου (firewall) με αρχιτεκτονική ενός υπολογιστή διαλογής (screened host).



Σχήμα 8-3: Πυρότοιχος με υπολογιστή διαλογής

8.1.3.3 ΥΠΟΔΙΚΤΥΟ ΔΙΑΛΟΓΗΣ (SCREENED SUBNET)

Είναι μια αρχιτεκτονική παρόμοια με την αρχιτεκτονική πυρότοιχου με υπολογιστή διαλογής (screened host) με τη διαφορά ότι χρησιμοποιείται επιπρόσθετα ένας δεύτερος δρομολογητής φιλτραρίσματος προκειμένου να διαχωρίσει τον οχυρωμένο και το δίκτυο που αυτός βρίσκεται από το υπόλοιπο εσωτερικό δίκτυο, παρέχοντας κατά τον τρόπο αυτό ένα επιπλέον επίπεδο ασφάλειας. Η αρχιτεκτονική αυτή φαίνεται στο σχήμα 8-4.



Σχήμα 8-4: Πυρότοιχος με αρχιτεκτονική υποδικτύου διαλογής

8.1.4 ΠΕΡΙΒΑΛΛΟΝ ΠΥΡΟΤΟΙΧΟΥ

Το «περιβάλλον» των πυρότοιχων είναι ένας όρος που χρησιμοποιείται για να περιγράψει το σύνολο των συστημάτων και συστατικών που εμπλέκονται στην παροχή ή την υποστήριξη της πλήρης λειτουργίας των πυρότοιχων σε ένα δεδομένο σημείο ενός δικτύου. Ένα απλό περιβάλλον πυρότοιχου μπορεί να περιλαμβάνει μόνο ένα πυρότοιχο φιλτραρίσματος πακέτων και τίποτα άλλο. Ένα πιο σύνθετο και ασφαλές περιβάλλον μπορεί να αποτελείται από διάφορους πυρότοιχους, εκπροσώπους (proxies) και από ειδικές τοπολογίες για την υποστήριξη των συστημάτων και της ασφάλειας. Ακολούθως παρουσιάζονται ορισμένα συστήματα και τοπολογίες δικτύων που χρησιμοποιούνται σε δημοφιλή περιβάλλοντα πυρότοιχων [NIST 800-41].

8.1.4.1 ΑΠΟΣΤΡΑΤΙΚΟΠΟΙΗΜΕΝΗ ΖΩΝΗ (DMZ)

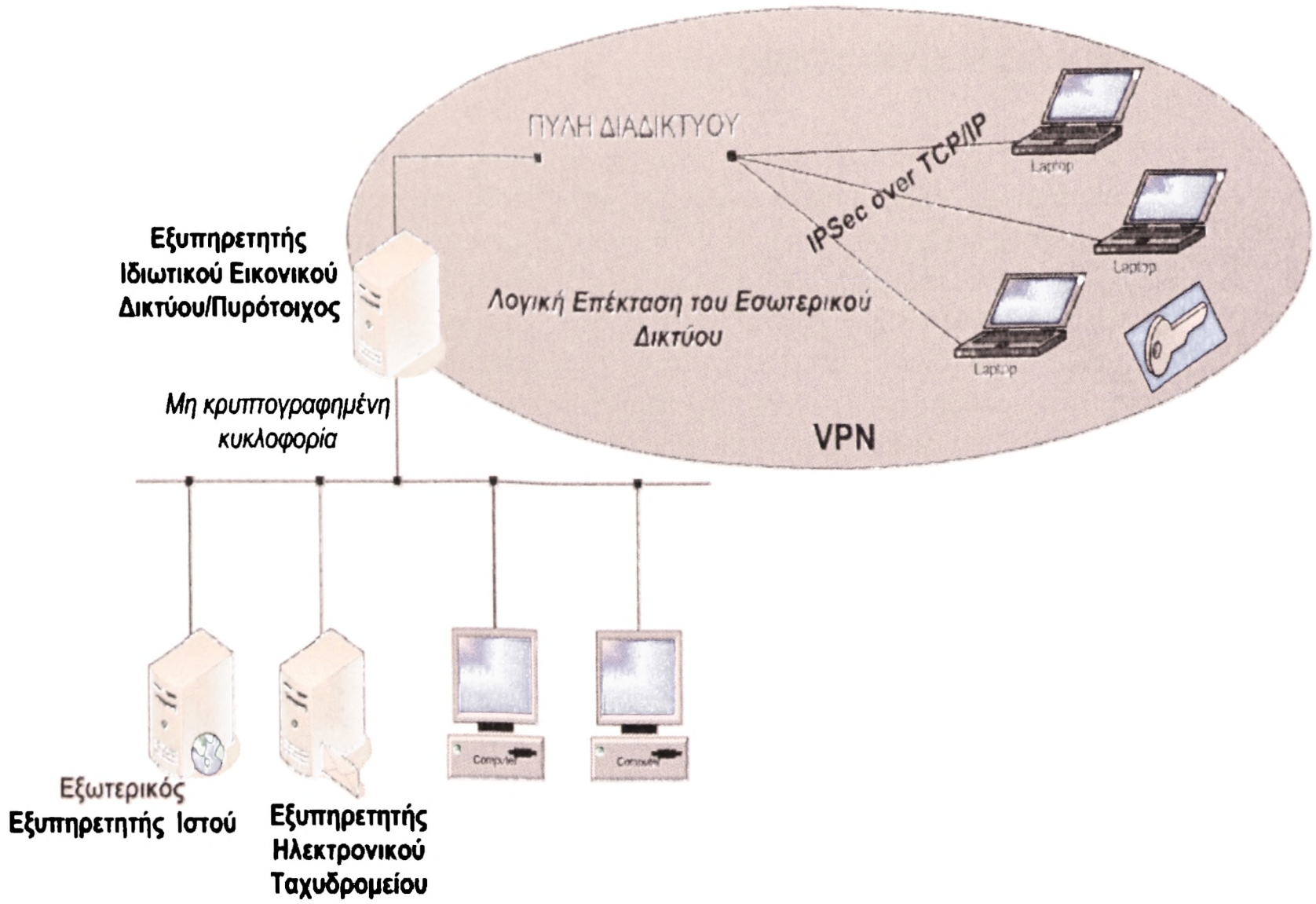
Η πιο κοινή εφαρμογή περιβάλλοντος πυρότοιχου (firewall) είναι γνωστή ως Αποστρατικοποιημένη Ζώνη (DMZ). (Βλέπε Κεφ. 7°, παράγραφο 7.1.2.1)

8.1.4.2 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ (VPNs)

Μια πολύτιμη χρήση για τους πυρότοιχους και τα περιβάλλοντα πυρότοιχων είναι η κατασκευή Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks – VPNs). Ένα ιδεατό ιδιωτικό δίκτυο κατασκευάζεται πάνω στα υπάρχοντα μέσα (media) και τα πρωτόκολλα δικτύων με τη χρησιμοποίηση επιπρόσθετων πρωτοκόλλων και συνήθως κρυπτογράφηση. Εάν το εικονικό ιδιωτικό δίκτυο είναι κρυπτογραφημένο μπορεί να χρησιμοποιηθεί ως επέκταση του εσωτερικού, προστατευμένου δικτύου. Στις περισσότερες περιπτώσεις, τα εικονικά ιδιωτικά δίκτυα χρησιμοποιούνται για να παρέχουν ασφαλείς συνδέσεις δικτύων δια μέσου δικτύων που δεν εμπιστεύονται. Παραδείγματος χάριν, η εικονική ιδιωτική τεχνολογία δικτύων χρησιμοποιείται όλο και περισσότερο στον τομέα της παροχής της μακρινής πρόσβασης (remote access) χρηστών στα δίκτυα οργανισμών μέσω του Διαδικτύου.

Με τη χρησιμοποίηση της εικονικής ιδιωτικής τεχνολογίας δικτύων, μια οργάνωση αγοράζει μια απλή σύνδεση στο Διαδίκτυο, και εκείνη η σύνδεση χρησιμοποιείται για να επιτρέψει στους χρήστες την απομακρυσμένη πρόσβαση σε διαφορετικά ιδιωτικά δίκτυα και πόρους. Αυτή η απλή σύνδεση με το Διαδίκτυο μπορεί επίσης να χρησιμοποιηθεί για να παρέχει πολλούς άλλους τύπους υπηρεσιών. Κατά συνέπεια, αυτός ο μηχανισμός θεωρείται οικονομικά αποδοτικός. Σε επίπεδο πρωτοκόλλου, υπάρχουν διάφορες πιθανές επιλογές για σύγχρονο εικονικό ιδιωτικό δίκτυο. Ένα παράδειγμα για ένα σύγχρονο εικονικό δίκτυο είναι η χρησιμοποίηση ενός συνόλου πρωτοκόλλων IPsec (ασφάλεια Πρωτοκόλλου Διαδικτύου).

Ένα παράδειγμα ενός εικονικού ιδιωτικού δικτύου φαίνεται στο σχήμα 8-5.



Σχήμα 8-5: Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network-VPN)

8.1.4.3 ΕΝΔΟΔΙΚΤΥΑ (INTRANETS)

Ένα ενδοδίκτυο (intranet) είναι ένα δίκτυο που χρησιμοποιεί τους ίδιους τύπους υπηρεσιών, εφαρμογών και πρωτοκόλλων σε μια εφαρμογή Διαδικτύου, χωρίς να περιλαμβάνει εξωτερική συνδεσιμότητα (external connectivity). Μέσα στο εσωτερικό δίκτυο (ενδοδίκτυο), πολλά μικρότερα ενδοδίκτυα (intranets) μπορούν να δημιουργηθούν με την χρήση των εσωτερικών πυρότοιχων. Για παράδειγμα, ένας οργανισμός μπορεί να προστατεύσει το προσωπικό του δίκτυό με ένα εσωτερικό πυρότοιχο και το προστατευμένο δίκτυο που προκύπτει μπορεί να αναφερθεί ως ένα προσωπικό ενδοδίκτυο. Δεδομένου ότι τα ενδοδίκτυα χρησιμοποιούν τα ίδια πρωτόκολλα και τις υπηρεσίες εφαρμογής που παρουσιάζονται στο διαδίκτυο, πολλά από τα ζητήματα ασφάλειας που παρουσιάζονται στις εφαρμογές Διαδικτύου παρουσιάζονται επίσης και στις εφαρμογές ενδοδικτύου.

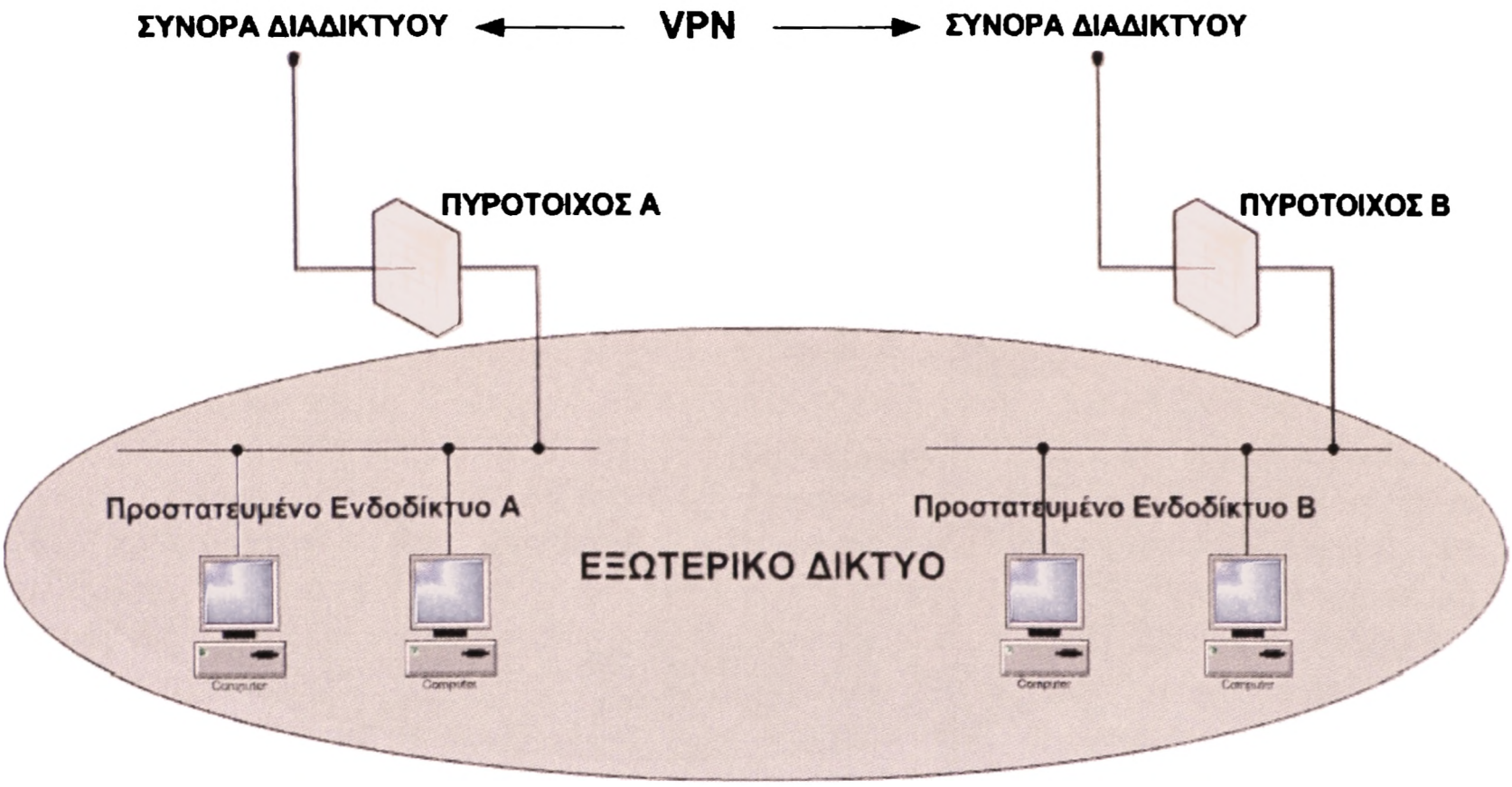
8.1.4.4 ΕΞΩΤΕΡΙΚΑ ΔΙΚΤΥΑ (EXTRANETS)

Τα εξωτερικά δίκτυα αποτελούν το τρίτο κομμάτι της σύγχρονης εικόνας της επιχειρηματικής συνδετικότητας. Ένα εξωτερικό δίκτυο είναι συνήθως ένα ενδοεπιχειρησιακό ενδοδίκτυο, δηλαδή δύο ενδοδίκτυα που ενώνονται μέσω του Διαδικτύου. Το εξωτερικό δίκτυο επιτρέπει την περιορισμένη, ελεγχόμενη απομακρυσμένη πρόσβαση remote access) στους χρήστες μέσω κάποιας μορφής επικύρωσης και κρυπτογράφησης όπως

παρέχεται μέσα από ένα εικονικό δίκτυο (VPN). Τα εξωτερικά δίκτυά έχει σχεδόν όλα τα χαρακτηριστικά των ενδοδικτύων, εκτός από το γεγονός ότι τα εξωτερικά δίκτυα σχεδιάζονται για να υπάρξουν έξω από ένα περιβάλλον πυρότοιχου.

Εξ ορισμού, ο σκοπός του εξωτερικού δικτύου είναι να παρέχει πρόσβαση στις ενδεχομένως ευαίσθητες πληροφορίες σε συγκεκριμένους μακρινούς χρήστες ή οργανισμούς και συγχρόνως την άρνηση της πρόσβασης σε εξωτερικούς χρήστες και συστήματα.

Πολλοί οργανισμοί και αντιπροσωπείες υιοθετούν αυτήν την περίοδο την τοπολογία των εξωτερικών δικτύων για να επικοινωνήσουν με τους πελάτες τους. Μέσα σε ένα εξωτερικό δίκτυο υπάρχουν πολλές διαθέσιμες επιλογές οι οποίες μπορούν να επιβάλλουν ποικίλους βαθμούς επικύρωσης, αναγραφής και κρυπτογράφησης. Στο παρακάτω σχήμα (σχήμα 8-6) απεικονίζεται ένα εξωτερικό εικονικό ιδιωτικό δίκτυο (extranet VPN) το οποίο ενώνει δυο ενδοδίκτυα (intranets).



Σχήμα 8-6: Εξωτερικό ιδιωτικό εικονικό δίκτυο ενώνει δυο ενδοδίκτυα

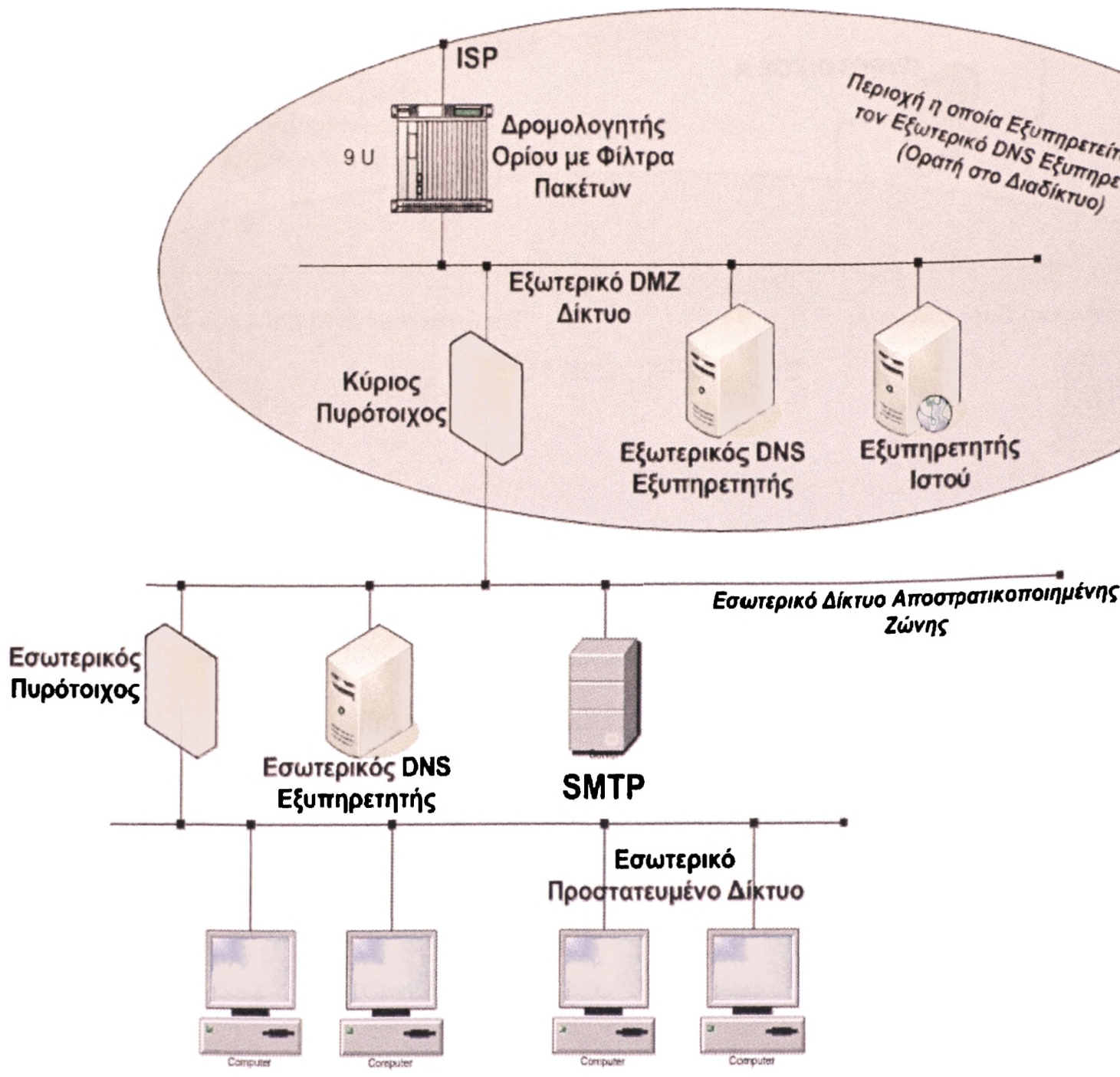
8.1.4.5 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems – IDS) σχεδιάστηκαν για να ενημερώνουν/ειδοποιούν και σε μερικές περιπτώσεις να αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση σε δικτυακά συστήματα και δικτυακούς πόρους. (Βλέπε Κεφ. 4, παράγραφο 4.6).

8.1.4.6 ΥΠΗΡΕΣΙΑ ΟΝΟΜΑΤΟΛΟΓΙΑΣ ΠΕΔΙΩΝ

Η Υπηρεσία Ονοματολογίας Πεδίων (Domain Name Service –DNS) είναι κρίσιμη για οποιοδήποτε περιβάλλον που χρησιμοποιεί το Διαδίκτυο. Λόγω της ευαίσθητης φύσης αυτής

της υπηρεσίας είναι απαραίτητο να εφαρμοστούν ειδικά μέτρα ασφάλειας. Κατ' αρχάς, οι εσωτερικοί εξυπηρετητές ονοματολογίας πεδίων (Domain Name Servers) πρέπει να κρατηθούν χωριστοί από τους εξωτερικούς εξυπηρετητές ονοματολογίας πεδίων. Παραδείγματος χάριν, ένας εξυπηρετητής ονοματολογίας πεδίων που είναι προσιτός σε ολόκληρο τον κόσμο δεν πρέπει να περιέχει εισόδους για τα συστήματα που δεν πρέπει να επικοινωνήσουν με τον εξωτερικό κόσμο, με μόνη πιθανή εξαίρεση τους επικυρωμένους μακρινούς χρήστες. Επιτρέποντας τέτοιες ιδιωτικές εισόδους να υπάρξουν σε έναν εξωτερικό εξυπηρετητή ονοματολογίας πεδίων χρησιμεύουν μόνο στο να παρέχουν έναν κατάλογο στόχων για έναν μακρινό επιτιθέμενο. Ένας οργανισμός πρέπει να διατηρήσει ξεχωριστά τους εσωτερικούς και εξωτερικούς εξυπηρετητές ονοματολογίας πεδίων. Αυτή η πρακτική, γνωστή ως Split DNS (Διαχωρισμός Εξυπηρετητών Ονοματολογίας Πεδίων), εξασφαλίζει ότι τα ιδιωτικά εσωτερικά συστήματα δεν είναι ποτέ αναγνωρίσιμα από ανθρώπους οι οποίοι βρίσκονται έξω από τον οργανισμό/επιχείρηση. Δεύτερον, είναι επίσης απαραίτητο να ελεγχθούν όλοι οι τύποι προσβάσεων που οποιοσδήποτε δεδομένος εξυπηρετητής ονοματολογίας πεδίων θα επιτρέψει.



Σχήμα 8-7: Παράδειγμα Διαχωρισμού Εξυπηρετητών Ονοματολογίας Πεδίων (Split DNS)

8.1.5 ΠΟΛΙΤΙΚΕΣ ΠΥΡΟΤΟΙΧΩΝ (FIREWALL POLICIES)

Η πολιτική ασφάλειας των πυρότοιχων υπαγορεύει πως ο πυρότοιχος θα πρέπει να χειριστεί εφαρμογές του Διαδικτύου όπως ο Ιστός (WEB), το ηλεκτρονικό ταχυδρομείο (E_MAIL), TELNET κ.λ.π. Η πολιτική ασφάλειας επίσης περιγράφει τον τρόπο με τον οποίο ένας πυρότοιχος θα πρέπει να διαχειρίζεται και να ενημερώνεται.

Χωρίς μια πολιτική πυρότοιχου οι διαχειριστές και οι οργανισμοί «κινούνται στα τυφλά». Οι πυρότοιχοι μπορεί να είναι σύνθετα και η διαχείρισή τους να είναι δύσκολη, ενώ προβλήματα ασφάλειας μπορούν να εμφανισθούν καθημερινά. Χωρίς την ύπαρξη μιας πολιτικής ασφάλειας η οποία θα καθοδηγήσει την υλοποίηση και τη διαχείριση των πυρότοιχων, οι πυρότοιχοι από μόνοι τους μπορεί να αποτελέσουν ένα σημαντικό πρόβλημα ασφάλειας για τον οργανισμό/επιχείρηση. Ακολούθως περιγράφονται ορισμένα σημαντικά σημεία όσον αφορά την πολιτική ασφάλειας των πυρότοιχων [NIST 800-41].

4.1.5.1 ΜΙΑ ΓΕΝΙΚΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Οι οργανισμοί και οι αντιπροσωπείες θα πρέπει να χρησιμοποιούν πυρότοιχους για να ασφαλίσουν τις Διαδικτυακές τους συνδέσεις καθώς επίσης και τις συνδέσεις τους με άλλα δίκτυα. Σε απομακρυσμένες τοποθεσίες οι χρήστες θα πρέπει να χρησιμοποιούν προσωπικούς πυρότοιχους και συσκευές πυρότοιχων για να ασφαλίσουν τις συνδέσεις τους με το Διαδίκτυο και με τους Παροχείς Υπηρεσιών Διαδικτύου (Internet Service Providers-ISPs). Οι οργανισμοί θα πρέπει να δουν τους πυρότοιχους σαν την πρώτη γραμμή άμυνας του οργανισμού έναντι των εξωτερικών απειλών. Η εσωτερική ασφάλεια θα πρέπει να είναι βασική προτεραιότητα του οργανισμού. Τα εσωτερικά συστήματα θα πρέπει να «μπαλώνονται» και να διαμορφώνονται έγκαιρα. Οι οργανισμοί θα πρέπει να ελέγχουν τις αναφορές της ομάδας ανταπόκρισης περιστατικών ασφάλειας (Incident Response Team) και ιστοχώρους σχετικούς με ζητήματα ασφάλειας (security websites) με σκοπό να συλλέξουν πληροφορίες σχετικά με τρέχουσες επιθέσεις και ευπάθειες. Η πολιτική ασφάλειας του πυρότοιχου θα πρέπει να ενημερώνεται μόνο όταν είναι απαραίτητο να ενημερωθεί, ανάλογα με τις ανάγκες του οργανισμού. Οι οργανισμοί θα πρέπει να αναγνωρίσουν ότι όλη η διαχείριση του συστήματος και ειδικότερα η διαχείριση των πυρότοιχων απαιτεί σημαντικό χρόνο και πολύ καλή εκπαίδευση. Οι οργανισμοί θα πρέπει να εξασφαλίσουν ότι οι διαχειριστές τους εκπαιδεύονται συχνά και μεθοδικά πάνω σε θέματα ασφάλειας έτσι ώστε να είναι ενήμεροι για τις πιο σύγχρονες απειλές και ευπάθειες ενός οργανισμού/επιχείρησης.

4.1.5.2 ΠΟΛΙΤΙΚΗ ΕΠΙΛΟΓΗΣ ΠΥΡΟΤΟΙΧΟΥ

Οι οργανισμοί θα πρέπει να εξετάσουν προσεκτικά ποιος πυρότοιχος η πιο περιβάλλον πυρότοιχων ταιριάζει καλύτερα με τις ανάγκες τους. Ένα περιβάλλον πυρότοιχων θα πρέπει να χρησιμοποιηθεί για να εκτελέσει τις ακόλουθες γενικές λειτουργίες:

- Φιλτράρισμα πακέτων και πρωτοκόλλων.
- Εκτέλεση διαδικασιών εκπροσώπων (proxies) σε επιλεγμένες εφαρμογές.
- Καταγραφή της κυκλοφορίας που επιτρέπεται ή που απαγορεύεται από τον πυρότοιχο.

- Παροχή πιστοποίησης στους χρήστες χρησιμοποιώντας μια μορφή πιστοποίησης που δεν βασίζεται σε στατικούς, επαναχρησιμοποιήσιμους κωδικούς οι οποίοι μπορούν να υποκλαπούν.

Ο πυρότοιχος θα πρέπει να είναι ικανό να φιλτράρει πακέτα βασιζόμενο στα ακόλουθα χαρακτηριστικά:

- Πρωτόκολλο, IP, ICMP (Internet Control Message Protocol) κ.λ.π.
- Τις IP διευθύνσεις πηγής και προορισμού.
- Τις θύρες (ports) πηγής και προορισμού (οι οποίες προσδιορίσουν τις εφαρμογές που είναι σε χρήση).
- Τη διασύνδεση του πυρότοιχου στον οποίο το πακέτο εισήχθη.

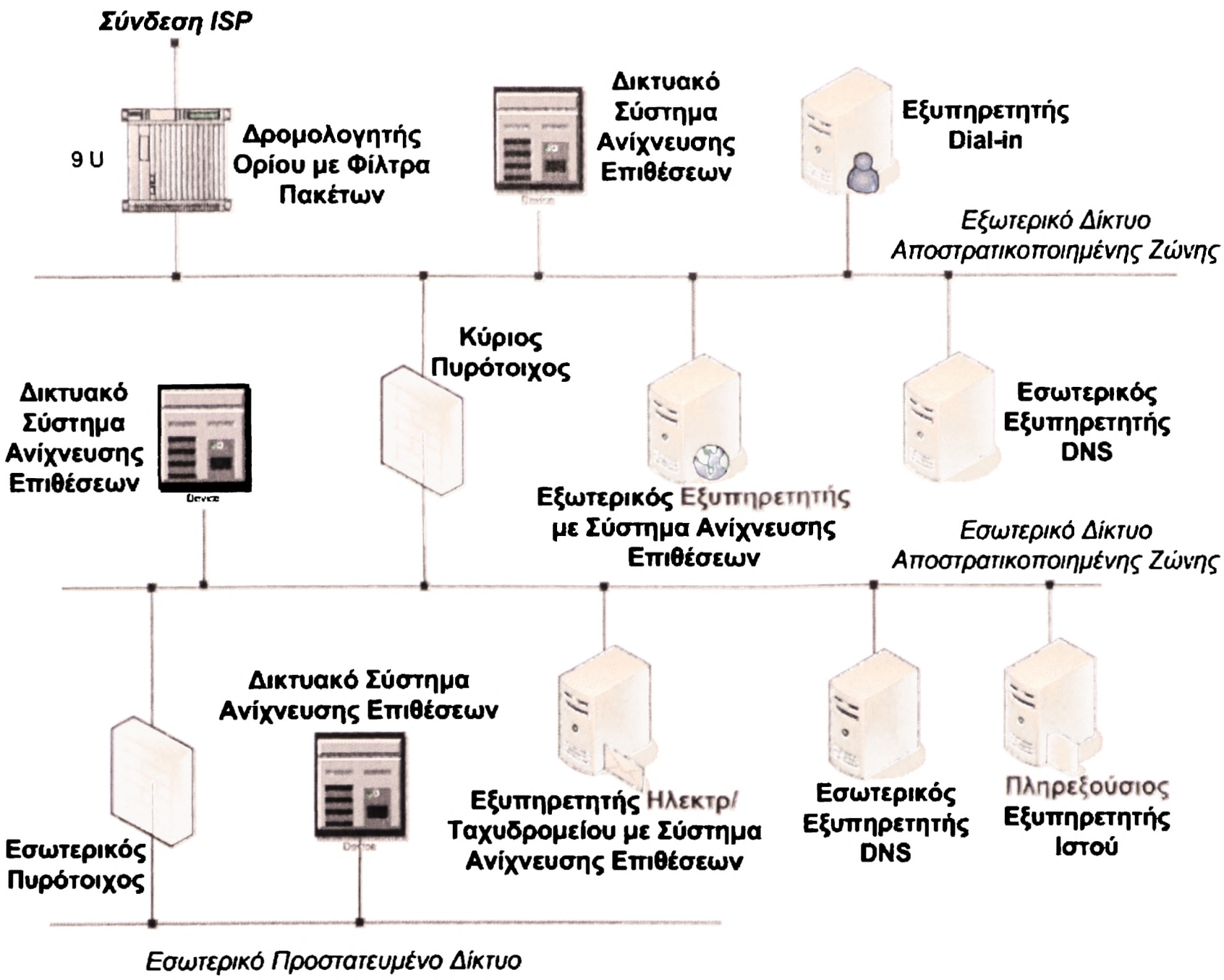
4.1.5.3 ΠΟΛΙΤΙΚΗ ΔΗΜΙΟΥΡΓΙΑΣ ΑΣΦΑΛΟΥΣ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΠΥΡΟΤΟΙΧΩΝ

Ένας δρομολογητής ορίου (boundary router) ή άλλος πυρότοιχος θα πρέπει να χρησιμοποιηθεί στην σύνδεση με το διαδίκτυο για να δημιουργήσει μια αποστρατικοποιημένη ζώνη (DMZ). Εξυπηρετητές Ιστού και άλλοι δημόσια προσβάσιμοι εξυπηρετητές θα πρέπει να τοποθετηθούν στην αποστρατικοποιημένη ζώνη έτσι ώστε αυτοί να μπορούν να είναι προσβάσιμοι όταν χρειάζεται ενώ παράλληλα θα προστατεύονται από τον πυρότοιχο. Οι εσωτερικοί χρήστες θα πρέπει να προστατεύονται με ένα επιπλέον πυρότοιχο.

Το σχήμα 8-8 δείχνει ένα γενικό περιβάλλον πυρότοιχων. Για τους μακρινούς χρήστες ένα ιδιωτικό εικονικό δίκτυο είναι προτιμότερο. Όταν ένας dial in εξυπηρετητής βρίσκεται πίσω από έναν πυρότοιχο, είναι πιο ασφαλές να συνδυαστεί με έναν εξυπηρετητή εικονικού ιδιωτικού δικτύου ο οποίος είναι τοποθετημένος σε έναν πυρότοιχο ή εξωτερικά ενός πυρότοιχου, έτσι ώστε οι μακρινές συνδέσεις να μπορούν με ασφάλεια να πιστοποιηθούν και να κρυπτογραφηθούν.

Η ανίχνευση εισβολών (intrusion detection) συνιστά μια πρόσθετη προστασία ενάντια στις επιθέσεις. Το σχήμα 8-8 απεικονίζει δικτυακά συστήματα ανίχνευσης εισβολών (network-based IDS) καθώς επίσης και συστήματα ανίχνευσης εισβολών που είναι εγκατεστημένα σε υπολογιστές (host-based IDS) τα οποία μπορούν να χρησιμοποιηθούν σε συστήματα στα οποία η ρυθμοαπόδοση (throughput) δεν αποτελεί σημαντικό ζήτημα. Η μετάφραση διευθύνσεων δικτύων και ο διαχωρισμός των εξυπηρετητών ονοματολογίας πεδίων (split DNS) χρησιμοποιούνται για να κρύψουν τα ονόματα και τις διευθύνσεις των εσωτερικών συστημάτων από εξωτερικά δίκτυα. Οι μακρινοί χρήστες θα πρέπει να χρησιμοποιούν προσωπικούς πυρότοιχους ή συσκευές πυρότοιχων όταν συνδέονται με τους Παροχείς Υπηρεσιών Διαδικτύου (ISPs), ανεξάρτητα με το αν χρησιμοποιούνται απλές dial in συνδέσεις ή συνδέσεις υψηλής ταχύτητας.

Ακολούθως απεικονίζεται ένα γενικό περιβάλλον πυρότοιχων το οποίο περιλαμβάνει όλα εκείνα τα χαρακτηριστικά τα οποία αναφέρονται παραπάνω (Υπηρεσία Ονοματολογίας Πεδίων, Συστήματα Ανίχνευσης Εισβολών, Αποστρατικοποιημένη Ζώνη, Εικονικά Ιδιωτικά Δίκτυα κ.λ.π).



Σχήμα 8-8: Γενικό περιβάλλον πυρότοιχου

4.1.5.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΥΡΟΤΟΙΧΩΝ

Μια γενική ανάλυση κινδύνου και μια ανάλυση κόστους οφέλους θα πρέπει να γίνει πάνω στις εφαρμογές δικτύων τις οποίες ένας οργανισμός ή μια αντιπροσωπεία έχει επιλέξει να χρησιμοποιήσει. Αποτέλεσμα αυτής της ανάλυσης είναι η δημιουργία μιας λίστας των δικτυακών εφαρμογών και των μεθόδων εκείνων που θα χρησιμοποιηθούν για να ασφαλίσουν αυτές τις εφαρμογές. Μια πολιτική πυρότοιχου θα πρέπει να γραφτεί, η οποία θα συμπεριλαμβάνει όλες τις δικτυακές εφαρμογές που θα χρησιμοποιηθούν. Αυτή η πολιτική θα πρέπει να διατηρείται και να ενημερώνεται συχνά καθώς προκύπτουν νέες επιθέσεις και ευπάθειες ή καθώς οι ανάγκες των οργανισμών από πλευράς δικτυακών εφαρμογών αλλάζουν. Όλοι οι πυρότοιχοι και οι πολιτικές ασφάλειας θα πρέπει να εξετάζονται λεπτομερώς και μεθοδικά τουλάχιστον κάθε τρίμηνο.

Η προεπιλεγμένη πολιτική για τους πυρότοιχους σχετικά με τον χειρισμό της εισερχόμενης κυκλοφορίας, θα πρέπει να μπλοκάρει/εμποδίζει όλα τα πακέτα και τις συνδέσεις εκτός από συγκεκριμένους τύπους κυκλοφορίας και συγκεκριμένες συνδέσεις οι οποίες ρητά επιτρέπονται. Αυτή η προσέγγιση είναι ασφαλέστερη από μια άλλη προσέγγιση η οποία χρησιμοποιείται πιο συχνά από διάφορους οργανισμούς και είναι η εξής:

επιτρέπονται όλοι οι τύποι κυκλοφορίας και όλες οι συνδέσεις εξ ορισμού και έπειτα μπλοκάρονται/εμποδίζονται συγκεκριμένοι τύποι κυκλοφορίας και συγκεκριμένες συνδέσεις.

Κατά γενικό κανόνα, οποιαδήποτε κυκλοφορία ή οποιοδήποτε πρωτόκολλο το οποίο δεν είναι απαραίτητο, π.χ που δεν χρησιμοποιείται ή που δεν χρειάζεται στον οργανισμό και/η αμφισβητείται από την πολιτική ασφάλειας, θα πρέπει να μπλοκάρεται με τη χρήση ενός εξυπηρετητή ορίου και μιας τεχνολογίας φιλτραρίσματος πακέτων. Αυτό θα έχει σαν αποτέλεσμα την μείωση του κινδύνου επίθεσης στον οργανισμό και τη δημιουργία ενός δικτυακού περιβάλλοντος με λιγότερη δικτυακή κυκλοφορία, το οποίο θα μπορεί να ελεγχθεί πιο εύκολα. Οι εφαρμογές των εκπροσώπων (proxies) θα πρέπει να χρησιμοποιούνται για εξωτερικές HTTP συνδέσεις και για εξερχόμενα/εισερχόμενα ηλεκτρονικά μηνύματα. Οι διαδικασίες αυτές θα πρέπει να είναι ικανές να εκτελέσουν τις παρακάτω λειτουργίες:

- Μπλοκάρισμα των Java applets και Java εφαρμογών.
- Φιλτράρισμα ActiveX και JavaScript.
- Μπλοκάρισμα συγκεκριμένων επεκτάσεων MIME (Multipurpose Internet Mail Extensions).
- Ανίχνευση για ιούς.

Μέσα από μια πολιτική ασφάλειας πυρότοιχων θα πρέπει πάντα να μπλοκάρονται οι ακόλουθοι τύποι δικτυακής κυκλοφορίας:

- Εισερχόμενη κυκλοφορία από μια μη πιστοποιημένη πηγή, με διεύθυνση προορισμού τον ίδιο τον πυρότοιχο.
- Εισερχόμενη κυκλοφορία με διεύθυνση πηγής (source address) η οποία δείχνει ότι το πακέτο δημιουργήθηκε από ένα δίκτυο, πίσω από τον πυρότοιχο.
- Εισερχόμενη κυκλοφορία από ένα μη πιστοποιημένο σύστημα πηγής που περιέχει SNMP (Simple Network Management Protocol) κυκλοφορία.
- Εισερχόμενη ή εξερχόμενη δικτυακή κυκλοφορία η οποία περιέχει διεύθυνση πηγής ή προορισμού π.χ την 127.0.0.1 (local host-τοπικός υπολογιστής).
- Εισερχόμενη ή εξερχόμενη δικτυακή κυκλοφορία η οποία περιέχει διεύθυνση πηγής ή προορισμού την 0.0.0.0.

4.1.5.5 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΠΥΡΟΤΟΙΧΟΥ

Εάν ο πυρότοιχος υλοποιείται σε ένα λειτουργικό σύστημα, το οποίο έχει αποκτήσει ο οργανισμός από κάποιο προμηθευτή (π.χ UNIX, Windows®), τότε το λειτουργικό σύστημα θα πρέπει να «απελευθερωθεί» από τις περιττές εφαρμογές και να ενισχυθεί ενάντια στις επιθέσεις. Όλα τα «μπαλώματα» θα πρέπει να γίνονται με έναν γρήγορο τρόπο δράσης. Θα πρέπει να δημιουργούνται σε καθημερινή, εβδομαδιαία και μηνιαία βάση αντίγραφα ασφάλειας του λογισμικού και των δεδομένων του συστήματος πυρότοιχων, ενώ είναι πολύ σημαντικό να υπάρχει πάντα έτοιμο ένα τουλάχιστον εφεδρικό σύστημα πυρότοιχων το οποίο θα αναλάβει δράση σε περίπτωση βλάβης του βασικού συστήματος. Οι πυρότοιχοι πρέπει να καταγράφουν (log) όλη τη δραστηριότητα και οι διαχειριστές των πυρότοιχων θα πρέπει να εξετάζουν αυτές τις καταγραφές καθημερινά.

Το Πρωτόκολλο Δικτυακής Ώρας (Network Time Protocol-NTP) ή άλλος κατάλληλος μηχανισμός θα πρέπει να χρησιμοποιηθεί για να συγχρονίσει τις καταγραφές με άλλα συστήματα καταγραφών όπως τα συστήματα ανίχνευσης εισβολών (IDS). Όλη η διαχείριση

του συστήματος πυρότοιχων θα πρέπει να γίνεται από ένα τοπικό τερματικό και όχι απομακρυσμένα. Μόνο ο διαχειριστής ασφάλειας θα πρέπει να έχει πρόσβαση στο τοπικό αυτό τερματικό. Σε περίπτωση που επιτραπεί η διαχείριση του πυρότοιχου από μακριά, μέσω αναξιόπιστου δικτύου, τότε θα πρέπει να χρησιμοποιηθεί απαραίτητα κρυπτογράφηση απ'άκρη σ'άκρη και τεχνικές ισχυρής πιστοποίησης (π.χ one time passwords κ.λ.π). Ένας οργανισμός θα πρέπει να είναι προετοιμασμένος να χειριστεί προβλήματα ασφάλειας τα οποία είναι αναπόφευκτα παρά την προστασία που προσφέρει το περιβάλλον πυρότοιχων. Θα πρέπει να δημιουργηθεί μια ομάδα ανταπόκρισης περιστατικών ασφάλειας η οποία θα βοηθήσει στην ανάλυση αυτών των περιστατικών και την άμεση αποκατάσταση του συστήματος.

ΚΕΦΑΛΑΙΟ 9ο

9.1 ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

9.1 ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

Αν και το ηλεκτρονικό ταχυδρομείο είναι μια από τις πιο διαδεδομένες εφαρμογές του Διαδικτύου, ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης ηλεκτρονικών μηνυμάτων δεν εγγυώνται τη διασφάλιση του προσωπικού απορρήτου του χρήστη ούτε και την ακεραιότητα της λειτουργίας του συστήματός του. Ακόμα και ένας εισβολέας με μικρή εμπειρία γνωρίζει πολύ καλά ότι η υποκλοπή των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι εξαιρετικά εύκολη υπόθεση. Η διαδικασία του ηλεκτρονικού ταχυδρομείου χωρίζεται σε δύο κύρια μέρη [NIST 800-45]: 1) τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, οι οποίοι προωθούν, διαβιβάζουν και αποθηκεύουν ηλεκτρονικά μηνύματα και 2) τους πελάτες (clients) οι οποίοι διασυνδέονται με τους χρήστες και τους επιτρέπουν να διαβάσουν, να συνθέσουν, να στείλουν και να αποθηκεύσουν ηλεκτρονικά μηνύματα. Μετά τους εξυπηρετητές Ιστού, οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου είναι τα τμήματα εκείνα του δικτύου ενός οργανισμού τα οποία αποτελούν τον πιο συχνό στόχο των επιτιθέμενων.

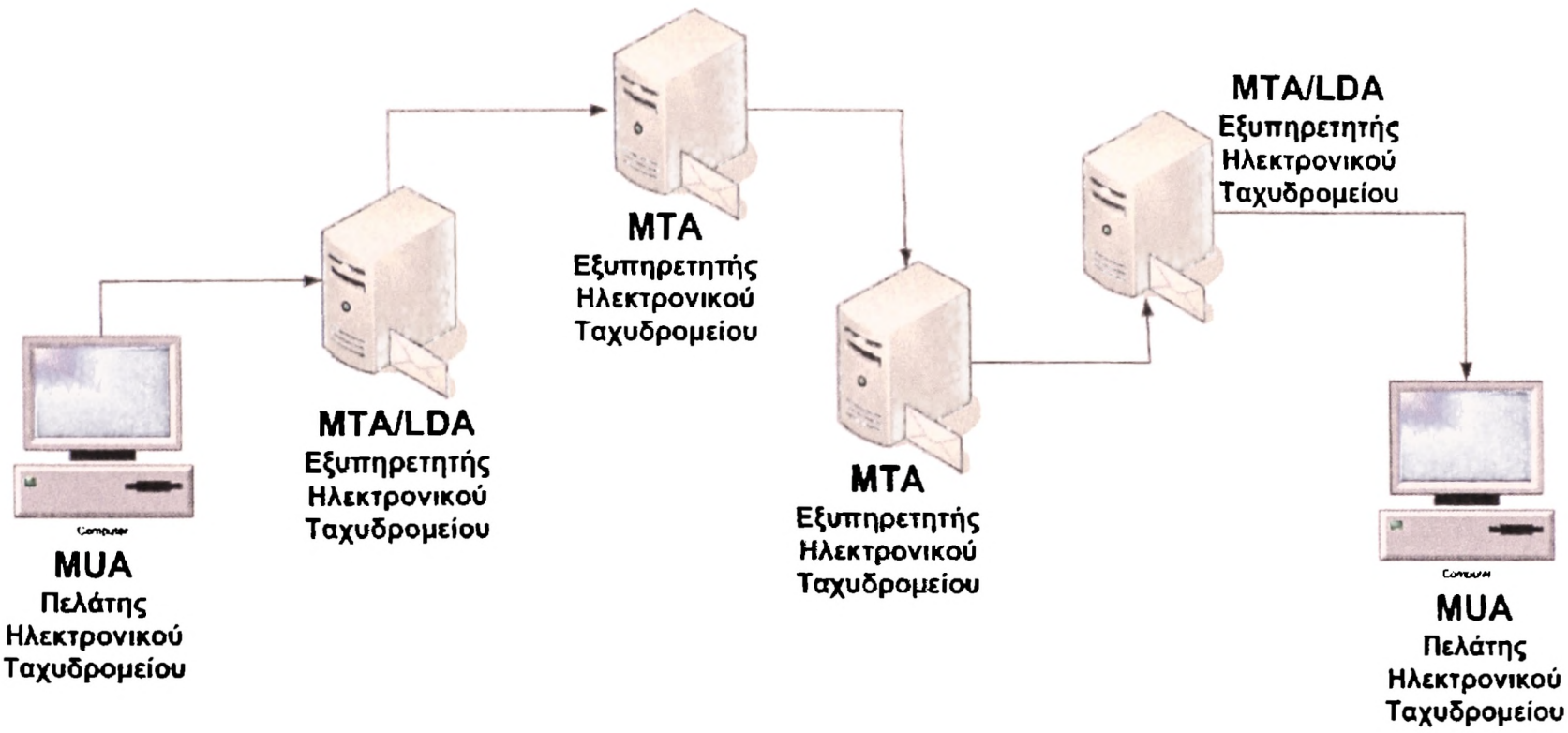
Για να γίνει κατανοητός ο όρος «ασφάλεια» του ηλεκτρονικού ταχυδρομείου είναι πολύ σημαντικό να γίνει κατανοητός ο τρόπος με τον οποίο τα ηλεκτρονικά μηνύματα συνθέτονται, παραδίδονται και αποθηκεύονται. Πολλοί χρήστες ηλεκτρονικού ταχυδρομείου πιστεύουν ότι μόλις συνθέσουν και στείλουν ένα μήνυμα, αυτό εμφανίζεται μαγικά στον υπολογιστή του παραλήπτη. Αυτό μπορεί να φαίνεται απλό αλλά στην πραγματικότητα ο χειρισμός και η παράδοση ενός μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να είναι διαδικασίες πολύπλοκες όπως συμβαίνει και στην περίπτωση του φυσικού ταχυδρομείου όπου το μήνυμα επεξεργάζεται και αρχειοθετείται σε διάφορες ενδιάμεσες θέσεις πριν φτάσει στον τελικό παραλήπτη.

Η διαδικασία ηλεκτρονικού ταχυδρομείου αρχίζει με την σύνθεση του μηνύματος. Οι πιο βασικοί πελάτες ηλεκτρονικού ταχυδρομείου ζητούν από τους χρήστες να ορίσουν τα ακόλουθα: το αντικείμενο του μηνύματος, το «σώμα» του μηνύματος και τους προοριζόμενους παραλήπτες. Όταν ο χρήστης συμπληρώσει αυτά τα πεδία και στείλει το μήνυμα, το μήνυμα μετασχηματίζεται σε μια συγκεκριμένη τυποποιημένη διάταξη [RFC 822]. Τα δυο πιο βασικά τμήματα ενός μηνύματος είναι η επικεφαλίδα και το «σώμα» του μηνύματος. Η επικεφαλίδα περιέχει κρίσιμες πληροφορίες σχετικά με το μήνυμα όπως η ημερομηνία, ο αποστολέας, ο/οι παραλήπτης/ες, η διαδρομή παράδοσης, το αντικείμενο του μηνύματος κ.λ.π. Το κύριο «σώμα» του μηνύματος περιέχει το πραγματικό περιεχόμενο του μηνύματος.

Όταν το μήνυμα μετασχηματιστεί σε μια τυποποιημένη διάταξη, μπορεί να μεταδοθεί. Χρησιμοποιώντας μια δικτυακή σύνδεση ο πελάτης ηλεκτρονικού ταχυδρομείου, ο οποίος αναφέρεται ως Αντιπρόσωπος Χρηστών Ηλεκτρονικού Ταχυδρομείου (Mail User Agent – MUA), συνδέεται με έναν Αντιπρόσωπο Μεταφοράς Μηνυμάτων (Mail Transport Agent – MTA) ο οποίος λειτουργεί στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Αφού αρχίσει η επικοινωνία, ο πελάτης ηλεκτρονικού ταχυδρομείου δίνει στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου την ταυτότητα του αποστολέα. Μετά ο πελάτης, χρησιμοποιώντας τις εντολές του εξυπηρετητή, λέει στον εξυπηρετητή ποιοι είναι οι προοριζόμενοι παραλήπτες του μηνύματος. Από αυτό το σημείο και μετά η παράδοση του μηνύματος βρίσκεται υπό τον έλεγχο του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.

Μόλις ο εξυπηρετητής αρχίζει και επεξεργάζεται το μήνυμα συμβαίνουν κάποια γεγονότα όπως: αναγνώριση του εξυπηρετητή του παραλήπτη, εγκατάσταση της σύνδεσης και μεταβίβαση του μηνύματος. Ο εξυπηρετητής του αποστολέα, χρησιμοποιώντας τις

υπηρεσίες ονοματολογίας πεδίων (DNS), καθορίζει τον/τους εξυπηρετητή/ες για τον/τους παραλήπτη/ες του μηνύματος. Κατόπιν ο εξυπηρετητής ανοίγει μια σύνδεση με τον/τους εξυπερετητή/ες του παραλήπτη και στέλνει το μήνυμα υιοθετώντας μια διαδικασία παρόμοια με αυτή που χρησιμοποιήθηκε από τον πελάτη. Σε αυτό το σημείο ένα από τα δύο παρακάτω γεγονότα μπορούν να συμβούν: εάν τα ταχυδρομικά κουτιά (mailboxes) του αποστολέα και του παραλήπτη βρίσκονται τοποθετημένα στον ίδιο εξυπηρετητή ηλεκτρονικού ταχυδρομείου, το μήνυμα παραδίδεται με τη χρησιμοποίηση ενός Τοπικού Αντιπροσώπου Παράδοσης (Local Delivery Agent-LDA). Εάν τα ταχυδρομικά κουτιά του αποστολέα και του παραλήπτη βρίσκονται τοποθετημένα σε διαφορετικούς εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τότε η διαδικασία της αποστολής του μηνύματος επαναλαμβάνεται από τον ένα αντιπρόσωπο μεταφοράς μηνυμάτων (MTA) στον άλλο μέχρι το μήνυμα να φτάσει στο ταχυδρομικό κουτί του παραλήπτη. Το παρακάτω σχήμα (σχήμα 9-1) απεικονίζει ένα παράδειγμα της ροής των μηνυμάτων.



Σχήμα 9-1: Παράδειγμα ροής μηνύματος

Κύριος φορέας των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι το Πρωτόκολλο Μεταφοράς Απλού Ταχυδρομείου (SMTP –Simple Mail Transfer Protocol). Το SMTP αναλαμβάνει τη μεταφορά μηνυμάτων από το μηχάνημα του χρήστη σε ένα εξυπηρετητή ηλεκτρονικού ταχυδρομείου, καθώς και την προώθηση του από έναν εξυπηρετητή ηλεκτρονικού ταχυδρομείου σε κάποιον άλλο. Κάθε εταιρεία παροχής υπηρεσιών Διαδικτύου (ISP –Internet Service Provider) διαθέτει έναν ή περισσότερους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την αποστολή των μηνυμάτων. Όταν ένας χρήστης συνδέεται μέσω τηλεφωνικής γραμμής με τον «παροχέα» του (ISP), μπορεί να «κατεβάσει» την αλληλογραφία του από τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου του «παροχέα» του, στον υπολογιστή του με τη βοήθεια του πρωτοκόλλου POP (Post Office Protocol) ή του IMAP (Internet Message Access Protocol).

Το ζήτημα ασφάλειας που προκύπτει κατά τη μετάδοση ενός μηνύματος ηλεκτρονικού ταχυδρομείου έγκειται στο γεγονός ότι τα πακέτα SMTP, τα οποία διέρχονται μέσω του δικτύου του «παροχέα» ή μέσω ενός εταιρικού δικτύου, είναι εν δυνάμει προσπελάσιμα από

οποιονδήποτε έχει πρόσβαση στο δίκτυο αυτό και χρησιμοποιεί ένα εργαλείο ανάλυσης δικτύων (network diagnostics tool ή sniffer). Εργαλεία του είδους είναι διαθέσιμα στο Διαδίκτυο και μάλιστα οποιοσδήποτε μπορεί να τα βρει σχετικά εύκολα. Βασική λειτουργία των sniffers είναι η υποκλοπή των πακέτων που διέρχονται από έναν κόμβο του δικτύου. Πολλά εργαλεία του είδους είναι ικανά να υποκλέπτουν πακέτα των περισσότερων δικτυακών πρωτοκόλλων, συμπεριλαμβανομένων των SMTP, POP και IMAP. Έτσι, ένας «αδιάκριτος» χρήστης μπορεί να υποκλέψει την ηλεκτρονική αλληλογραφία, χρησιμοποιώντας ένα πρόγραμμα για «sniffing».

9.1.1 MIME ΚΑΙ S/MIME

9.1.1.1 MIME

Το ηλεκτρονικό ταχυδρομείο του Διαδικτύου επιτρέπει σε χρήστες από όλο τον κόσμο να ανταλλάσσουν μηνύματα. Τον Ιούνιο του 1992, ένα νέο πρωτόκολλο του Διαδικτύου καθιερώθηκε, το MIME, το οποίο είναι το ακρωνύμιο της αγγλικής φράσης *Multipurpose Internet Mail Extensions.* Το MIME και προσφέρει έναν τρόπο για την ανταλλαγή κειμένου σε γλώσσες εκτός της αγγλικής και μηνυμάτων πολυμέσων μεταξύ διαφορετικών υπολογιστικών συστημάτων. Συγκεκριμένα, ένα μήνυμα συμβατό του MIME μπορεί να περιέχει:

- Πολλαπλά αντικείμενα.
- Κείμενο με απεριόριστο μήκος και απεριόριστο μήκος γραμμών.
- Σύνολα χαρακτήρων πέρα από το US - ASCII, επιτρέποντας τη σύνταξη μηνυμάτων σε διάφορες γλώσσες.
- Εμπλουτισμένο κείμενο, χρήση δηλαδή διάφορων τυπογραφικών στοιχείων *(fonts).*
- Εικόνα, κινούμενη εικόνα, ήχο.
- Δυαδικά αρχεία ή αρχεία εφαρμογών *(tar files, postscript files).*
- Δείκτες σε αρχεία αποθηκευμένα σε άλλους υπολογιστές.

Κάθε έγγραφο που ανταλλάσσεται μέσω του Διαδικτύου μπορεί να περιέχει πρόσθετα αρχεία των οποίων τα περιεχόμενα μπορεί να είναι γραφικά, ήχος, video, κλπ. Όταν ένας εξυπηρετητής Ιστού στέλνει ένα έγγραφο σε κάποιο πρόγραμμα πλοήγησης ενσωματώνει στο μήνυμα πληροφορίες που περιγράφουν τον τύπο των αρχείων αυτών σε μια κεφαλίδα σύμφωνα με το MIME πρωτόκολλο. Το πρόγραμμα-παραλήπτης χρησιμοποιεί αυτή την πληροφορία της κεφαλίδας για να αναγνωρίσει τον τύπο του αρχείου. Στην ουσία η κεφαλίδα είναι συμπληρωματική πληροφορία που τοποθετείται στην αρχή του μηνύματος. Οι πληροφορίες-δεδομένα βρίσκονται στο σώμα (body) του μηνύματος.

Στην κεφαλίδα κάθε μηνύματος ενσωματώνεται ένας τύπος και ένας υπό-τύπος. Ο τύπος καθορίζει γενικά το είδος του περιεχομένου, ενώ ο υπό-τύπος τον εξειδικεύει (π.χ. Type: image, subtype: jpg). Οι τύποι και οι υπό-τύποι γράφονται στην κεφαλίδα στο πεδίο Content-Type. Για την αναγνώριση του τύπου και του υπό-τύπου χρησιμοποιείται η κατάληξη του ονόματος ενός αρχείου. Για παράδειγμα για ένα αρχείο του MS Word στην κεφαλίδα θα γραφεί: Content-Type: application/msword.

Ακολούθως απεικονίζεται ένας περιληπτικός πίνακας (πίνακας 9-Α) επικεφαλίδων του πρωτοκόλλου MIME.

	Επικεφαλίδες	Περιγραφή
1	MIME-Version	Αριθμός έκδοσης του MIME.
2	Content-Type	Καθορίζει το είδος των δεδομένων.
3	Content-Transfer-Encoding	Η κωδικοποίηση των δεδομένων.
4	Content-ID Content-Description	Επιπλέον περιγραφή και ταυτοποίηση των δεδομένων

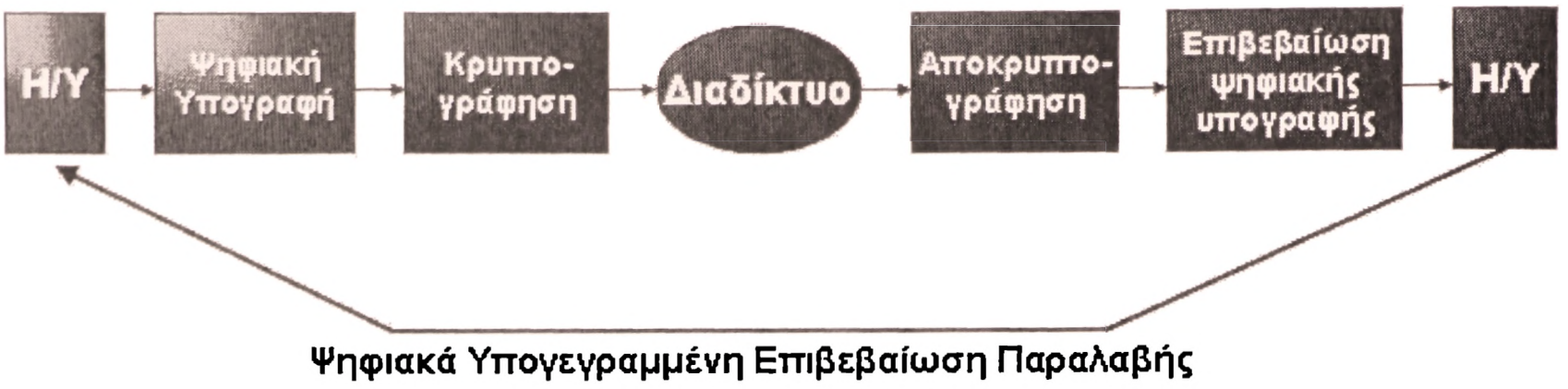
Πίνακας 9-Α: Επικεφαλίδες του πρωτοκόλλου MIME

Όπως έχει αποδειχθεί, το λογισμικό που εφαρμόζει το MIME πρωτόκολλο μπορεί να προκαλέσει πολλά προβλήματα. Τα πιο σημαντικά από αυτά έχουν να κάνουν με τα postscript (*η PostScript είναι μια γλώσσα προγραμματισμού που προορίζεται για περιγραφή εγγράφων και είναι βελτιστοποιημένη για εκτυπώσεις γραφικών και κειμένου. Χρησιμοποιείται κυρίως στους εκτυπωτές laser, αλλά τη συναντούμε και σε καταγραφικά σχεδίων (plotters), μηχανές φωτοστοιχειοθεσίας (image setters) και άλλες συσκευές εξόδου*) προγράμματα. Γνωστά παραδείγματα είναι η χρήση τους για την αλλαγή των κωδικών σε εκτυπωτές postscript με αποτέλεσμα την άρνηση εξυπηρέτησης και την αυθαίρετη διαχείριση αρχείων. Πρέπει επίσης να τονιστεί ότι τα ηλεκτρονικά μηνύματα του Διαδικτύου δεν είναι ασφαλή, αφού υπηρεσίες όπως η πιστοποίηση ταυτότητας και η ακεραιότητα δεδομένων δεν παρέχονται από τα πρωτόκολλα SMTP και MIME. Για να αντιμετωπιστούν τα προαναφερόμενα προβλήματα ασφαλείας αναπτύχθηκε ένα νέο πρωτόκολλο με επεκτάσεις ασφαλείας. Το νέο αυτό πρωτόκολλο ονομάζεται S/MIME (Secure-MIME) και αποτελεί εξειδίκευση του πρωτοκόλλου MIME.

9.1.1.2 S/MIME

Το S/MIME όπως έχει ήδη αναφερθεί αποτελεί μια εξειδίκευση του πρωτοκόλλου MIME και αναπτύχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων. Σκοπός του είναι η καταπολέμηση της πλαστογραφίας και της υποκλοπής ηλεκτρονικών μηνυμάτων με ταυτόχρονη διατήρηση της ευκολίας στη χρήση. Σχεδιάστηκε ώστε να μπορεί εύκολα να ενοποιηθεί σε προϊόντα ηλεκτρονικού ταχυδρομείου, επεκτείνοντας το πρωτόκολλο MIME σύμφωνα με ένα σύνολο κρυπτογραφικών τυποποιήσεων (*Public Key Cryptography Standards – PKCS).* Η παγκόσμια υιοθέτηση του S/MIME θα ωφελήσει τους χρήστες, αφού έννοιες όπως η ακεραιότητα των δεδομένων, η αυθεντικότητα και η διαφύλαξη του απόρρητου των συναλλαγών θα είναι διαθέσιμες σε όλους. Το S/MIME δίνει τη δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να

αποκρυπτογραφηθεί από ένα άλλο. Στο σχήμα 9-2 φαίνεται ο τρόπος λειτουργίας του S/MIME. Επίσης το S/MIME προσφέρει ένα σύνολο από προαιρετικές υπηρεσίες ασφάλειας οι οποίες είναι οι εξής:



Σχήμα 9-2: Τρόπος λειτουργίας του S/MIME

- **Υπογεγραμμένες Αποδείξεις Παραλαβής (Signed Receipts)**
  Η επιστροφή μιας υπογεγραμμένης απόδειξης παραλαβής παρέχει στον αποστολέα εξασφάλιση της παραλαβής του μηνύματος και του επιτρέπει να αποδείξει σε τρίτο ότι ο παραλήπτης ήταν σε θέση να επαληθεύσει την υπογραφή του αρχικού μηνύματος. Η αίτηση επιστροφής απόδειξης επιτυγχάνεται με την τοποθέτηση της ιδιότητας αποστολής απόδειξης στο πεδίο SignerInfo. Φυσικά, η ιδιότητα αποστολής απόδειξης μπορεί να ζητηθεί μόνον εφόσον το μήνυμα είναι ψηφιακά υπογεγραμμένο.

- **Ετικέτες Ασφαλείας (Security Labels)**
  Ετικέτα ασφαλείας είναι ένα σύνολο πληροφοριών ασφαλείας που αφορούν στο βαθμό ασφαλείας των περιεχομένων. Μπορούν να περιγράφουν επίπεδα ασφάλειας («μυστικό», «απόρρητο», «περιορισμένη πρόσβαση», κτλ.) ή να περιγράφουν ομάδες ανθρώπων που μπορούν να έχουν πρόσβαση στην πληροφορία (π.χ. «γιατροί», «ασφαλιστικές εταιρίες», «ασθενείς», «όλοι»).

- **Διαχείριση Λιστών Ηλεκτρονικού Ταχυδρομείου (Mail List Management)**
  Τα προγράμματα ηλεκτρονικού ταχυδρομείου πρέπει να δημιουργούν κρυπτογραφημένα μηνύματα με διαφορετική δομή για κάθε παραλήπτη και συνεπώς ο φόρτος εργασίας αυξάνεται σημαντικά για μεγάλο αριθμό παραληπτών που ανήκουν στην ίδια ταχυδρομική λίστα. Για το λόγο αυτό, συστήματα που καλούνται Mail List Agents (MLAs) αναλαμβάνουν την ανά χρήστη διαχείριση του μηνύματος. Με τον τρόπο αυτό διευκολύνεται η αποστολή μηνυμάτων σε μεγάλες ταχυδρομικές λίστες. Ένας MLA παρουσιάζεται στον αποστολέα ως ένας τυπικός αποδέκτης, ενώ στην πραγματικότητα λειτουργεί ως ένα σημείο περαιτέρω επεξεργασίας του μηνύματος που διανέμει το μήνυμα σε όλα τα μέλη της ταχυδρομικής λίστας. Επίσης, ένας MLA πρέπει να αντιμετωπίζει τους λεγόμενους «βρόχους ηλεκτρονικού ταχυδρομείου» (mail loops). Βρόχος Ηλεκτρονικού Ταχυδρομείου είναι μια κατάσταση που εμφανίζεται όταν μια ταχυδρομική λίστα είναι μέλος μιας δεύτερης που και αυτή με τη σειρά της είναι μέλος της πρώτης.

- **Ιδιότητα Υπογεγραμμένου Πιστοποιητικού (Signing Certificate Attribute)**
  Σημαντικά προβλήματα έχουν παρουσιαστεί λόγω του γεγονότος ότι τα πιστοποιητικά του υπογράφοντος δεν ασφαλίζονται μαζί με τις υπογεγραμμένες ιδιότητες ενός μηνύματος. Η

εκμετάλλευση αυτού του ελαττώματος έχει οδηγήσει στην ανάπτυξη τεχνικών «επίθεσης» που έχουν ως στόχο την αντικατάσταση του πιστοποιητικού. Η ιδιότητα υπογεγραμμένου πιστοποιητικού έχει σκοπό να αποτρέψει τις επιθέσεις αυτές. Η ιδιότητα αυτή προστίθεται στις υπογεγραμμένες ιδιότητες και περιλαμβάνει στοιχεία που ταυτοποιούν το σωστό πιστοποιητικό. Συγκεκριμένα, η συνάρτηση κατακερματισμού (hash) του πιστοποιητικού περιλαμβάνεται στις υπογεγραμμένες ιδιότητες παρέχοντας επιπλέον ασφάλεια. Εάν η συνάρτηση κατακερματισμού στις υπογεγραμμένες ιδιότητες δεν ταιριάζει με τη συνάρτηση κατακερματισμού του λαμβανόμενου πιστοποιητικού, τότε η υπογραφή θεωρείται άκυρη.

9.1.2 PRETTY GOOD PRIVACY – PGP

Το PGP είναι ένα πακέτο λογισμικού το οποίο χρησιμοποιείται ευρύτατα στο Διαδίκτυο για την επίτευξη ασφαλούς μετάδοσης μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το PGP είναι ένα ισχυρό λογισμικό κρυπτογράφησης που επιτρέπει στους χρήστες να επικοινωνούν με ασφάλεια. Επίσης, τους παρέχει τη δυνατότητα προστασίας των αρχείων τους. Η αυθεντική έκδοση του λογισμικού PGP αναπτύχθηκε από τον Philip Zimmermann το 1991 και εξαπλώθηκε ραγδαία στο Διαδίκτυο [Zimm00]. Πρόκειται για ένα προϊόν στρατηγικής σημασίας. Κύριο μέλημα του Zimmermann ήταν να δημιουργήσει ένα προϊόν ασφάλειας ικανό να εμποδίσει την κυβέρνηση και τους άλλους οργανισμούς να εισβάλλουν στην ιδιωτικότητα των χρηστών του λογισμικού, κάτι που έως τότε πραγματοποιούταν με μεγάλη ευκολία. Ο Zimmermann αναγνώρισε την μεγάλη ανάγκη που έχει ο απλός πολίτης για ισχυρά μέσα προστασίας της ιδιωτικότητάς του παρατηρώντας:

- Την ανάπτυξη βάσεων δεδομένων μεγάλου όγκου προσωπικών πληροφοριών.
- Τη σύνδεση των βάσεων δεδομένων μέσω των ευρέως διαδεδομένων δικτύων.
- Την ευκολία με την οποία κάποιος μπορεί να παρακολουθήσει, να αποθηκεύσει και να επεξεργαστεί πληροφορίες που διακινούνται σε δίκτυα.
- Τη μακρά ιστορία από λανθασμένους χειρισμούς μηχανισμών υπηρεσιών (όπως η CIA).

Στην επίτευξη του στόχου του Zimmermann για ένα προϊόν ασφάλειας κατάλληλο για όλους συνετέλεσε και το γεγονός ότι η τεχνολογία είναι πια προσιτή στον καθένα που επιθυμεί να απομακρύνει τα «αδιάκριτα βλέμματα».

Το PGP διατίθεται δωρεάν για προσωπική χρήση, όμως απαιτείται άδεια για τη χρησιμοποίηση του σε εμπορικές εφαρμογές. Το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT) λειτουργεί ως κέντρο προώθησης του λογισμικού που προορίζεται για προσωπική χρήση σε συνεργασία με τον Zimmermann ο οποίος ίδρυσε και μια ομώνυμη με το λογισμικό, εταιρία (Pretty Good Privacy, Inc.) για να προωθήσει την εμπορική έκδοση του λογισμικού. Σκοπός του PGP ήταν η χρήση του σε συνδυασμό με το σύστημα ηλεκτρονικού ταχυδρομείου που προϋπήρχε και είναι συμβατό με σχεδόν κάθε πλατφόρμα. Η βασική ιδέα του PGP ήταν ότι είναι ανώφελο να επιχειρήσει κάποιος να εμποδίσει την εξέταση πληροφοριών που διακινούνται σε δίκτυα μέσω του ηλεκτρονικού ταχυδρομείου ή κάποιου άλλου μέσου επικοινωνίας. Έτσι, η μοναδική μορφή προστασίας είναι η εξασφάλιση ότι τα δεδομένα που παρακολουθούνται είναι ακατανόητα σε όλους τους άλλους εκτός από τους νόμιμους παραλήπτες τους. Αυτό επιτυγχάνεται με ισχυρή κρυπτογράφηση.

9.1.2.1 ΣΥΣΤΑΤΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ PGP

Το PGP αποτελείται από τέσσερα στοιχεία κρυπτογράφησης και έναν αριθμό συστατικών μερών λογισμικού, συμβατών μεταξύ τους. Ο πυρήνας των μηχανισμών ασφάλειας είναι:

1. Ο αλγόριθμος κρυπτογράφησης δεδομένων IDEA (International Data Encryption Algorithm).
2. Το σύστημα κρυπτογράφησης δημοσίου κλειδιού RSA για τη διαχείριση κλειδιών.
3. Η συνάρτηση κατακερματισμού MD5.
4. Μια γεννήτρια τυχαίων αριθμών.

Τα άλλα συστατικά του PGP υλοποιούν τυπικές λειτουργίες όπως, για παράδειγμα, την αλληλεπίδραση με το χρήστη, τη διαχείριση αρχείων και τη συμπίεση των δεδομένων.

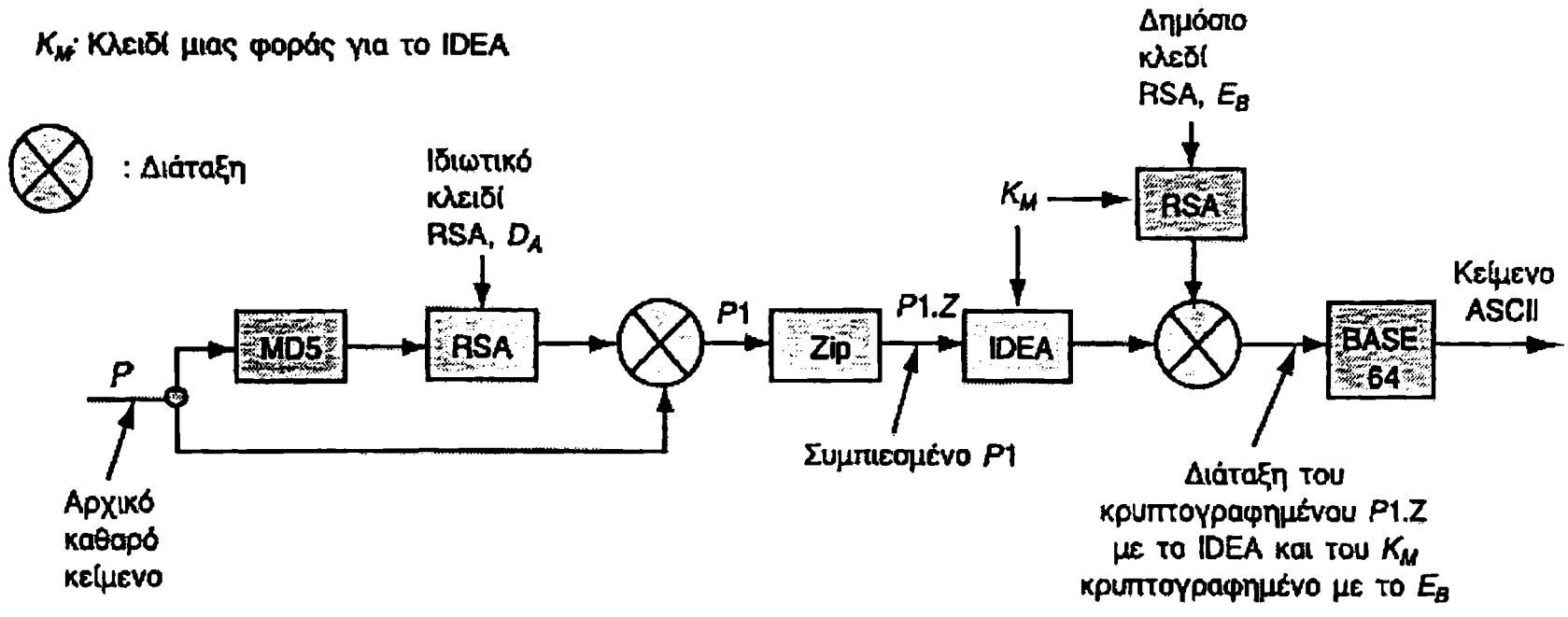
9.1.2.2 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ PGP

Για να κατανοήσουμε την λειτουργία του PGP θεωρούμε ότι υπάρχουν δυο χρήστες και ο χρήστης Α θέλει να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, *P*, στον Β. Οι δύο χρήστες έχουν τα δικά τους ιδιωτικά (D_x) και δημόσια (Εχ) κλειδιά RSA και θεωρούμε ότι ο ένας γνωρίζει το δημόσιο κλειδί του άλλου.

1. Αρχικά, το πρόγραμμα PGP στον υπολογιστή του Α περνάει το μήνυμα, *P*, από τη συνάρτηση κατακερματισμού (hash) MD5.
2. Στη συνέχεια, το hash κρυπτογραφείται με το ιδιωτικό RSA κλειδί του Α, D_A. Όταν ο Β τελικά λάβει το μήνυμα, τότε θα μπορέσει να αποκρυπτογραφήσει το hash με το δημόσιο κλειδί, E_A, και να επιβεβαιώσει ότι είναι σωστό.
3. Κατόπιν, το κρυπτογραφημένο hash και το αρχικό μήνυμα διατάσσονται σε ένα νέο μήνυμα *P1* και συμπιέζονται ώστε να παραχθεί το *PX.Z*.
4. Στη συνέχεια, παράγεται τυχαία ένα κλειδί για τον αλγόριθμο IDEA, K_M, το οποίο ισχύει μόνο για τη συγκεκριμένη αποστολή ηλεκτρονικού ταχυδρομείου. Το κλειδί αυτό χρησιμοποιείται για τη κρυπτογράφηση του *P1.Z* με το IDEA.
5. Επιπλέον, το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του Β.
6. Τα δύο αυτά τμήματα διατάσσονται και αποστέλλονται στο δίκτυο.
7. Όταν ο Β λάβει το μήνυμα, αποκρυπτογραφεί το κλειδί K_M χρησιμοποιώντας το ιδιωτικό του κλειδί RSA (D_B).
8. Χρησιμοποιώντας το K_M αποκρυπτογραφεί το μήνυμα που είναι κρυπτογραφημένο με τον αλγόριθμο IDEA και λαμβάνει το *P1.Z*.
9. Μετά την αποσυμπίεση ο Β ξεχωρίζει το hash από το καθαρό μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Α.
10. Αν το hash συμφωνεί με τον υπολογισμό MD5 που εκτελεί ο ίδιος, τότε γνωρίζει ότι το μήνυμα είναι αυτό που έστειλε ο Α.

Στην παραπάνω διαδικασία, ο χρονοβόρος υπολογισμός με τον αλγόριθμο RSA χρησιμοποιείται μόνο για την κρυπτογράφηση των κλειδιών συνόδου, που έχουν πολύ μικρότερο μέγεθος από το συνολικό μήνυμα. Για το μήνυμα χρησιμοποιήθηκε ο αλγόριθμος

IDEA που είναι αρκετές τάξεις μεγέθους πιο γρήγορος. Στο παρακάτω σχήμα (σχήμα 9-3) απεικονίζεται σχηματικά η λειτουργία του PGP.



Σχήμα 9-3: Σχηματική αναπαράσταση της λειτουργίας του PGP

9.1.3 S/MIME vs PGP

Η επιλογή μεταξύ PGP και S/MIME είναι δύσκολη και εξαρτάται από πολλούς παράγοντες. Οι νεότερες εμπορικές εκδόσεις του PGP έχουν προσθέσει κάποιες ιδιαίτερες λειτουργίες προκειμένου να μπορέσει να ανταγωνιστεί το S/MIME, καθιστώντας έτσι πιο δύσκολη την επιλογή μεταξύ των δύο αυτών πρωτοκόλλων. Ακολούθως αναφέρονται ορισμένα πλεονεκτήματα των PGP και S/MIME.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ PGP:

1. Είναι κατάλληλο για μικρές ομάδες η απλούς χρήστες

2. Είναι ασφαλέστερο με την υποστήριξη για AES, αν και το S/MIME δεν απέχει και πολύ.

3. Υπάρχουν διαθέσιμες δωρεάν εκδόσεις λογισμικού.

4. Δεν απαιτεί (αλλά υποστηρίζει εάν είναι απαραίτητο) εξωτερική υποδομή δημοσίου κλειδιού. (Το S/MIME απαιτεί από έναν οργανισμό να αγοράσει πιστοποιητικά ή να εγκαταστήσει την δική της αρχή πιστοποίησης).

5. Μπορεί να χρησιμοποιηθεί, αν και με περισσότερα βήματα, από οποιαδήποτε εφαρμογή πελατών ηλεκτρονικού ταχυδρομείου.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ S/MIME:

1. Είναι κατάλληλο για μεγάλες ομάδες χρηστών η μεγάλους οργανισμούς.

2. Χρησιμοποιεί το πιο ευρέως συμβατό πρότυπο κρυπτογράφησης ηλεκτρονικού ταχυδρομείου.

3. Παρέχει περισσότερη διαφάνεια στον τελικό χρήστη.

9.1.4 ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΚΑΙ ΘΩΡΑΚΗΣΗΣ ΕΝΟΣ ΕΞΥΠΗΡΕΤΗΤΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Ο όρος «ασφάλεια» θα πρέπει να ληφθεί υπόψη από το αρχικό στάδιο προγραμματισμού και από την αρχή του κύκλου ζωής ανάπτυξης των συστημάτων προκειμένου να μεγιστοποιηθεί η ασφάλεια και να ελαχιστοποιηθούν οι δαπάνες. Στα στάδια προγραμματισμού ενός εξυπηρετητή ηλεκτρονικού ταχυδρομείου τα ακόλουθα στοιχεία θα πρέπει να εξεταστούν:

☞ Προσδιορισμός του σκοπού του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.

- Ποιες κατηγορίες πληροφοριών θα επεξεργάζονται η θα μεταδίδονται μέσω του εξυπηρετητή;
- Ποιες είναι οι απαιτήσεις ασφάλειας για αυτές τις πληροφορίες;
- Ποιες άλλες υπηρεσίες θα παρέχονται από τον εξυπηρετητή; (γενικά η ύπαρξη ενός υπολογιστή ο οποίος θα λειτουργεί *μόνο* ως εξυπηρετητής ηλεκτρονικού ταχυδρομείου είναι η πιο ασφαλής επιλογή).
- Ποιες είναι οι απαιτήσεις ασφάλειας για αυτές τις πρόσθετες υπηρεσίες;
- Σε ποιο σημείο του δικτύου θα τοποθετηθεί ο εξυπηρετητής;

☞ Προσδιορισμός των δικτυακών εφαρμογών που θα παρέχονται από τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου, όπως εκείνες που παρέχονται μέσω των ακόλουθων πρωτοκόλλων:

- Send Message Transfer Protocol – SMTP.
- Post Office Protocol – POP.
- Internet Message Access Protocol – IMAP.

☞ Προσδιορισμός οποιουδήποτε λογισμικού υπηρεσιών δικτύου, πελάτη και εξυπηρετητή, που εγκαθίσταται στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου ή σε άλλους εξυπηρετητές υποστήριξης.

☞ Προσδιορισμός των χρηστών ή τις κατηγορίες των χρηστών που χρησιμοποιούν τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου ή άλλους υπολογιστές υποστήριξης.

☞ Καθορισμός των προνομίων που θα έχει κάθε κατηγορία χρηστών πάνω στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου και σε άλλους υπολογιστές υποστήριξης.

- ☞ Λήψη απόφασης σχετικά το αν και πως οι χρήστες θα πιστοποιούνται και πως θα προστατευθούν τα δεδομένα πιστοποίησης.

- ☞ Καθορισμός του τρόπου με τον οποίο θα επιβληθεί η κατάλληλη πρόσβαση στις πηγές πληροφοριών.

- ☞ Καθορισμός σχετικά με το ποιες εφαρμογές των εξυπηρετητών ηλεκτρονικού ταχυδρομείου θα καλύψουν τις ανάγκες του οργανισμού. Εδώ θα πρέπει να ληφθούν υπόψη τα παρακάτω ζητήματα:

  - Το κόστος.
  - Συμβατότητα με υπάρχουσα υποδομή.
  - Η γνώση των υπαρχόντων υπαλλήλων.
  - Η υπάρχουσα σχέση με τους προμηθευτές.
  - Το ιστορικό σχετικά με τις ευπάθειες.
  - Λειτουργικότητα.

- ☞ Κοντινή συνεργασία με τους προμηθευτές κατά τη διάρκεια του σταδίου προγραμματισμού του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.

Η διαδικασία επιλογής της/των εφαρμογής/ών του εξυπηρετητή μπορεί επίσης να καθορίσει και την επιλογή του λειτουργικού συστήματος που θα χρησιμοποιηθεί. Ωστόσο, στο βαθμό που είναι εφικτό, οι διαχειριστές του εξυπηρετητή ηλεκτρονικού ταχυδρομείου θα πρέπει να επιλέξουν εκείνο το λειτουργικό σύστημα το οποίο θα πρέπει να παρέχει τα ακόλουθα:

- ☞ Ελάχιστη έκθεση σε ευπάθειες.
- ☞ Ικανότητα να θέσει εκτός λειτουργίας τις περιττές δικτυακές υπηρεσίες οι οποίες μπορεί να είναι ενσωματωμένες στο λειτουργικό σύστημα ή στο λογισμικό του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.
- ☞ Ικανότητα να καταγράφει τις κατάλληλες δραστηριότητες του εξυπηρετητή με σκοπό να ανιχνεύσει εισβολές που έχουν συμβεί ή αποπειραθείσες εισβολές.
- ☞ Ικανότητα να αρνείται την πρόσβαση σε πληροφορίες του εξυπηρετητή, εκτός από τις πληροφορίες εκείνες οι οποίες προορίζονται να είναι διαθέσιμες (η πολιτική ασφάλειας καθορίζει ποίες πληροφορίες είναι διαθέσιμες και ποιες όχι).

9.1.5 ΑΣΦΑΛΗΣ ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΔΙΑΜΟΡΦΩΣΗ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Μόλις ένα λειτουργικό σύστημα εγκατασταθεί, είναι κρίσιμο να εφαρμοστούν οποιαδήποτε «μπαλώματα» ή βελτιώσεις που θα διορθώσουν τις γνωστές ευπάθειες. Όλα τα λειτουργικά συστήματα που κυκλοφορούν σήμερα έχουν μερικές γνωστές ευπάθειες που πρέπει να διορθωθούν πριν χρησιμοποιηθεί το λειτουργικό σύστημα για να «φιλοξενήσει» έναν εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Για να ανιχνευθούν επαρκώς και να διορθωθούν αυτές οι ευπάθειες, οι διαχειριστές του εξυπηρετητή ηλεκτρονικού ταχυδρομείου θα πρέπει:

- Να δημιουργήσουν και να εφαρμόσουν μια διαδικασία επιδιόρθωσης.
- Να προσδιορίσουν τις ευπάθειες και τα εφαρμόσιμα «μπαλώματα».
- Να μετριάσουν τις ευπάθειες (μέχρι τα μπαλώματα να είναι διαθέσιμα, να δοκιμαστούν και να εγκατασταθούν).
- Να εγκαταστήσουν μόνιμες επιδιορθώσεις (που συχνά αποκαλούνται μπαλώματα, hotfixes, πακέτα υπηρεσιών ή ενημερώσεις).

Για καλύτερα αποτελέσματα ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου θα πρέπει να εγκατασταθεί σε έναν υπολογιστή ενός σκοπού, δηλαδή σε έναν υπολογιστή ο οποίος θα λειτουργεί *μόνο* ως εξυπηρετητής ηλεκτρονικού ταχυδρομείου. Κατά τη διαμόρφωση του λειτουργικού συστήματος πρέπει να τεθούν εκτός λειτουργίας όλα εκτός από εκείνα που επιτρέπονται ρητώς – δηλαδή να τεθούν εκτός λειτουργίας ή κατά προτίμηση να αφαιρεθούν όλες οι υπηρεσίες και οι εφαρμογές και έπειτα επιλεκτικά να επιτραπούν εκείνες οι υπηρεσίες και εφαρμογές που απαιτούνται από τον εξυπηρετητή ταχυδρομείου. Εάν είναι δυνατόν θα πρέπει να εγκατασταθεί η ελάχιστη διαμόρφωση λειτουργικού συστήματος που απαιτείται για την εφαρμογή εξυπηρετητή ταχυδρομείου με την επιλογή «ελάχιστη εγκατάσταση» (εάν είναι διαθέσιμη), ώστε να ελαχιστοποιηθεί η προσπάθεια που απαιτείται για την αφαίρεση των περιττών υπηρεσιών. Μερικές υπηρεσίες και εφαρμογές που πρέπει συνήθως να τεθούν εκτός λειτουργίας περιλαμβάνουν τα εξής:

- Windows NetBIOS / διανομή αρχείων και εκτυπωτών (μπορεί να μην είναι δυνατό σε όλες τις εγκαταστάσεις)
- Σύστημα αρχείων δικτύων (NFS)
- TELNET
- Απλό πρωτόκολλο διαχείρισης δικτύων (SNMP – Simple Network Management Protocol) (εάν δεν απαιτείται)
- Πρωτόκολλο Μεταφοράς Αρχείων (FTP - File Transfer Protocol)
- Σύστημα πληροφοριών δικτύων (NIS – Network Information System)
- Μεταγλωττιστές γλώσσας και βιβλιοθήκες
- Εργαλεία ανάπτυξης συστημάτων
- Εργαλεία διαχείρισης και χρησιμότητες δικτύων (εάν δεν απαιτείται).

Η αφαίρεση των περιττών υπηρεσιών και εφαρμογών είναι προτιμότερη από το να τεθούν απλά εκτός λειτουργίας μέσω των ρυθμίσεων διαμόρφωσης, επειδή οι επιθέσεις που προσπαθούν να αλλάξουν τις ρυθμίσεις και να ενεργοποιήσουν μια απενεργοποιημένη υπηρεσία δεν μπορούν να επιτευχθούν όταν έχουν αφαιρεθεί εντελώς τα λειτουργικά συστατικά. Η αφαίρεση ή η απενεργοποίηση των περιττών υπηρεσιών ενισχύει την ασφάλεια ενός εξυπηρετητή ταχυδρομείου με διάφορους τρόπους:

- Άλλες υπηρεσίες δεν μπορούν να εκτεθούν και να χρησιμοποιηθούν για να επιτεθούν στον υπολογιστή ή να βλάψουν τις υπηρεσίες του εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Κάθε υπηρεσία που προστίθεται σε έναν υπολογιστή αυξάνει τον κίνδυνο έκθεσης για εκείνο τον υπολογιστή επειδή κάθε υπηρεσία είναι μια άλλη πιθανή δίοδος πρόσβασης για έναν επιτιθέμενο.
- Ο υπολογιστής μπορεί να διαμορφωθεί ώστε να ταιριάξει με τις απαιτήσεις μιας συγκεκριμένης υπηρεσίας. Οι διαφορετικές υπηρεσίες μπορεί να απαιτούν διαφορετικό υλικό και λογισμικό διαμόρφωσης, οι οποίες θα μπορούσαν να οδηγήσουν σε περιττές ευπάθειες ή σε δυσμενείς επιπτώσεις στην απόδοση.

- Με τη μείωση των υπηρεσιών, ο αριθμός των Log καταχωρήσεων μειώνεται, επομένως η ανίχνευση απροσδόκητης συμπεριφοράς γίνεται ευκολότερη.

9.1.6 ΑΣΦΑΛΗΣ ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ ΕΞΥΠΗΡΕΤΗΤΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Από πολλές απόψεις, η ασφαλής εγκατάσταση και διαμόρφωση του λειτουργικού συστήματος θα καθρεφτίσει τη διαδικασία του λειτουργικού συστήματος. Η βασική αρχή είναι να εγκατασταθούν οι ελάχιστες υπηρεσίες που απαιτούνται από τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου και να εξαλειφθούν όλες οι γνωστές ευπάθειες μέσω των βελτιώσεων και των «μπαλωμάτων». Οποιεσδήποτε περιττές εφαρμογές και υπηρεσίες που έχουν εγκατασταθεί θα πρέπει να αφαιρεθούν αμέσως μόλις ολοκληρωθεί η διαδικασία εγκατάστασης. Κατά τη διάρκεια εγκατάστασης του εξυπηρετητή οι ακόλουθες ενέργειες θα πρέπει να εκτελεσθούν:

- Εγκατάσταση του λογισμικού του εξυπηρετητή σε έναν υπολογιστή ενός σκοπού, ο οποίο θα λειτουργεί μόνο ως εξυπηρετητής ηλεκτρονικού ταχυδρομείου.
- Εγκατάσταση ελάχιστων υπηρεσιών διαδικτύου που απαιτούνται.
- Εφαρμογή των κατάλληλων «μπαλωμάτων» και βελτιώσεων για να διορθώσουν τις γνωστές ευπάθειες.
- Αφαίρεση ή απενεργοποίηση όλων των υπηρεσιών που έχουν εγκατασταθεί από την εφαρμογή του εξυπηρετητή ηλεκτρονικού ταχυδρομείου και οι οποίες δεν απαιτούνται/χρειάζονται (FTP, απομακρυσμένη πρόσβαση, κ.λ.π).
- Απενεργοποίηση των επικίνδυνων ή περιττών εντολών ηλεκτρονικού ταχυδρομείου.
- Αφαίρεση οποιονδήποτε αρχείων παραδείγματος ή δοκιμής από τον εξυπηρετητή.
- Εφαρμογή του κατάλληλου προτύπου ασφάλειας στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου.

9.1.7 ΠΡΟΣΤΑΣΙΑ ΑΠΟ «ΜΟΧΘΗΡΟ ΚΩΔΙΚΑ»

Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται όλο και περισσότερο ως μέσο για την αποστολή δυαδικών αρχείων υπό μορφή συνημμένων. Αρχικά, αυτό δεν αποτέλεσε μεγάλο κίνδυνο ασφάλειας επειδή τα συνημμένα ήταν συνήθως μικρά έγγραφα επεξεργασίας κειμένου ή φωτογραφίες. Στη συνέχεια όμως καθώς οι περισσότεροι οργανισμοί άρχισαν να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο για καθημερινή συνεργασία, το μέγεθος και οι τύποι των συνημμένων του ηλεκτρονικού ταχυδρομείου αυξήθηκαν. Σήμερα, πολλά μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονται με μορφή συνημμένων όπως εκτελέσιμα προγράμματα, εικόνες, μουσική και ήχοι. Το κύριο ζήτημα που ένας οργανισμός πρέπει να αντιμετωπίσει είναι ποιους τύπους συνημμένων θα επιτρέψει.

Η απόφαση για το αν θα επιτραπεί η όχι ένα συνημμένο είναι αρκετά δύσκολη. Μην επιτρέποντας τα συνημμένα θα απλοποιούσε σίγουρα ένα σύστημα και θα το καθιστούσε ασφαλέστερο, ωστόσο θα μείωνε πιθανώς τη χρησιμότητά του σε έναν οργανισμό και οι χρήστες θα μπορούσαν απλά να υιοθετήσουν τα τεχνάσματα της κωδικοποίησης για να

εργαστούν γύρω από τον περιορισμό προκειμένου «να γίνει η δουλειά τους». Ωστόσο πολλοί είναι οι οργανισμοί οι οποίοι λόγω των καθημερινών αναγκών τους για επικοινωνία επιλέγουν να επιτρέψουν τουλάχιστον μερικά συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου. Με βάση την υπόθεση ότι τα συνημμένα ηλεκτρονικού ταχυδρομείου είναι επιθυμητά, ο διαχειριστής του εξυπηρετητή ηλεκτρονικού ταχυδρομείου πρέπει να καθορίσει ποιοι τύποι συνημμένων θα επιτραπούν. Η απλούστερη προσέγγιση είναι να επιτραπούν όλοι οι τύποι συνημμένων. Εάν αυτό συμβεί, κατόπιν θα πρέπει να εγκατασταθεί κάποιο είδος ανιχνευτή ιών μέσα στην διαδρομή διέλευσης ταχυδρομείου ώστε να φιλτράρει γνωστούς κακόβουλους κώδικες και ίσως ακόμη και κάποια χρησιμότητα φραξίματος συμπεριφοράς στον πελάτη για να αποτρέψει οποιεσδήποτε ανεπιθύμητες διαδικασίες από την εμφάνιση εκτελέσιμων συνημμένων. Μια καλύτερη προσέγγιση είναι να φιλτραριστούν οι ενδεχομένως επικίνδυνοι τύποι συνημμένων (π.χ., vbs, ws, wsc επεκτάσεις αρχείων) στον εξυπηρετητή ταχυδρομείου ή στην πύλη ταχυδρομείου κατά τη διάρκεια της διεξαγωγής ανίχνευσης ιών στους επιτρεπόμενους τύπους αρχείων.

Οι ιοί ή τα σκουλήκια μπορούν να διαβιβαστούν στα ηλεκτρονικά ταχυδρομεία υπό μορφή ιών ηλεκτρονικού ταχυδρομείου ή ιών συνημμένων. Εάν ένας εξυπηρετητής ταχυδρομείου δεν έχει εγκαταστήσει λογισμικό αντιιών ή το λογισμικό είναι αναποτελεσματικό τότε αυτό οδηγεί σε πιθανές αυξήσεις απειλής ασφάλειας ηλεκτρονικού ταχυδρομείου για τον τελικό χρήστη.

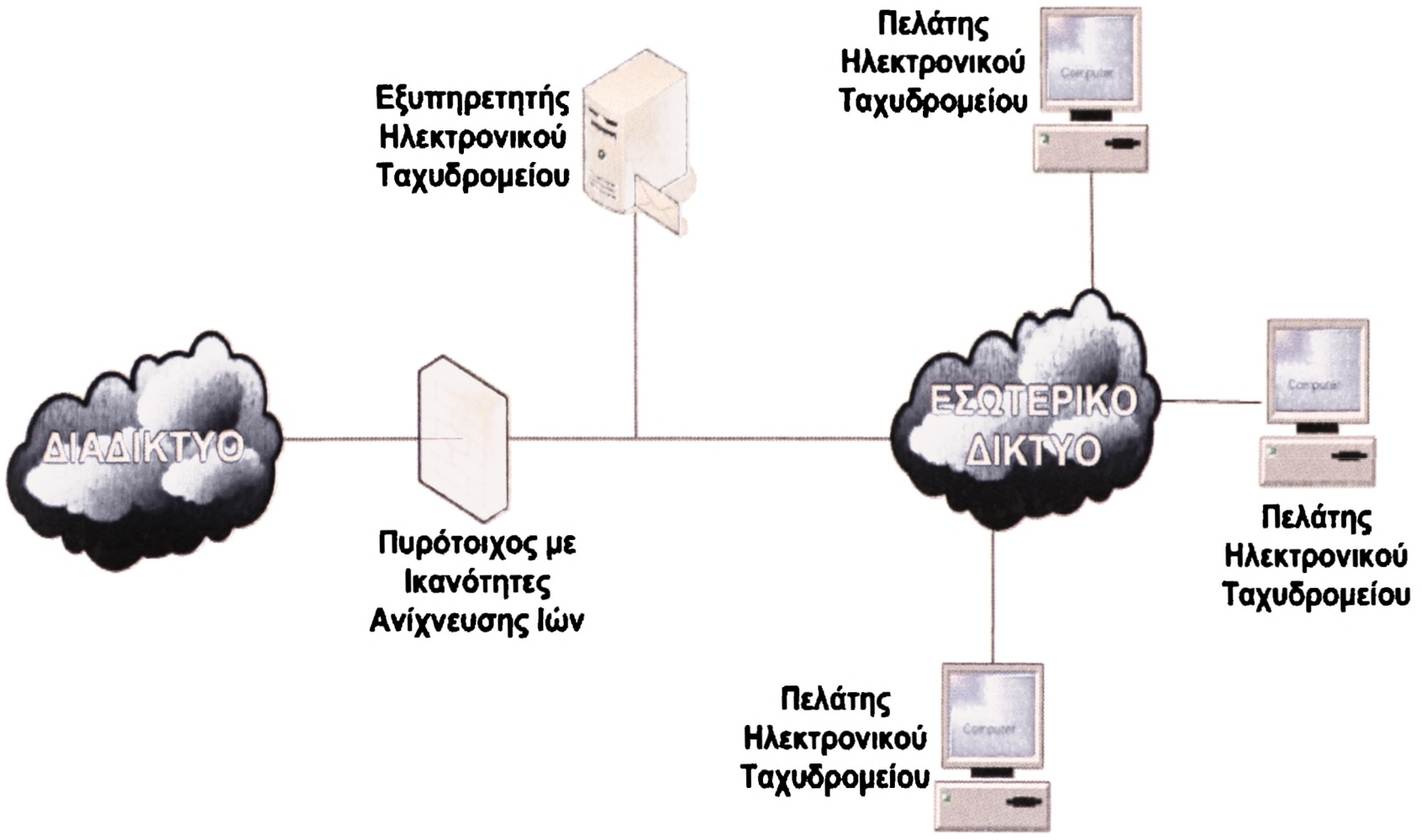
Για την προστασία από ιούς και άλλο κακόβουλο κώδικα είναι απαραίτητο να εφαρμοστεί η ανίχνευση σε ένα ή περισσότερα σημεία μέσα στη διαδικασία παράδοσης ηλεκτρονικού ταχυδρομείου. Η ανίχνευση ιών μπορεί να εφαρμοστεί στο φράγμα ασφάλειας καθώς το στοιχείο ταχυδρομείου εισάγεται στο δίκτυο του οργανισμού, στον εξυπηρετητή ταχυδρομείου ή στον υπολογιστή του τελικού χρήστη. Κάθε επιλογή έχει τα πλεονεκτήματα και τις αδυναμίες της. Εάν οι πόροι το επιτρέπουν, η χρησιμοποίηση περισσότερων του ενός αυτών των επιλογών μπορεί να παρέχει τη μεγαλύτερη ασφάλεια ελαχιστοποιώντας μερικές από τις αδυναμίες. Η ανίχνευση ιών στο φράγμα ασφάλειας είναι μια δημοφιλής επιλογή. Σε αυτήν την περίπτωση, το φράγμα ασφάλειας παρεμποδίζει τα μηνύματα προτού να φθάσουν στον εξυπηρετητή ταχυδρομείου του οργανισμού. Ο πυρότοιχος (firewall) ανιχνεύει κάθε μήνυμα και εάν δεν βρίσκεται κανένας ιός, διαβιβάζει το μήνυμα προς τον εξυπηρετητή ταχυδρομείου (σχήμα 9-4). Τα πλεονεκτήματα της ανίχνευσης ιών στο φράγμα ασφάλειας είναι τα εξής:

- Το ηλεκτρονικό μήνυμα μπορεί να ανιχνευθεί και στις δυο κατευθύνσεις (εισερχόμενο και εξερχόμενο από το δίκτυο του οργανισμού).
- Οι ιοί μπορούν να μπλοκαριστούν πριν εισέλθουν στο δίκτυο του οργανισμού.
- Η ανίχνευση του εισερχόμενου μηνύματος μπορεί να υλοποιηθεί με ελάχιστες αλλαγές στην υπάρχουσα διαμόρφωση του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.
- Δίδεται η δυνατότητα κεντρικής διαχείρισης της διαδικασίας ανίχνευσης των ηλεκτρονικών μηνυμάτων με στόχο να εξασφαλιστεί η συμμόρφωση με την πολιτική ασφάλειας του οργανισμού και η σωστή εφαρμογή και ενημέρωση του αντι-ιοικού λογισμικού.
- Τα φράγματα ασφάλειας υποστηρίζουν πολλαπλά πρωτόκολλα, έτσι η εφαρμογή των ανιχνευτών μπορεί επίσης να χρησιμοποιηθεί για να ανιχνεύσει άλλα πρωτόκολλα όπως το Πρωτόκολλο Μεταφοράς Υπερκειμένων (HTTP), το Πρωτόκολλο Μεταφοράς Αρχείων (FTP) κ.λ.π.

Τα μειονεκτήματα ανίχνευσης ιών στο φράγμα ασφάλειας είναι τα εξής:

- Απαιτείται σημαντική τροποποίηση της διαμόρφωσης του εξυπηρετητή ηλεκτρονικού ταχυδρομείου για την ανίχνευση των εξερχόμενων ηλεκτρονικών μηνυμάτων.
- Δεν μπορούν να ανιχνευθούν κρυπτογραφημένα μηνύματα.
- Δεν προσφέρει καμία προστασία στους εσωτερικούς χρήστες όταν ένας ιός βρίσκεται στο εσωτερικό δίκτυο του οργανισμού, εκτός αν το δίκτυο είναι διαμορφωμένο έτσι ώστε η κυκλοφορία SMTP δρομολογείται μέσω ενός ειδικού (αφιερωμένου) ανιχνευτή πριν φτάσει στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου.
- Απαιτούνται ισχυροί και ακριβοί εξυπηρετητές για να χειριστούν το φορτίο ενός μεγάλου οργανισμού.

Στο παρακάτω σχήμα απεικονίζεται η διαδικασία ανίχνευσης ιών η οποία υλοποιείται στο φράγμα ασφάλειας.



Σχήμα 9-4: Υλοποίηση συστήματος ανίχνευσης ιών στον πυρότοιχο

Μια δεύτερη επιλογή είναι η τοποθέτηση του ανιχνευτή ιών ηλεκτρονικού ταχυδρομείου στον ίδιο τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου (σχήμα 9-4). Αυτή η επιλογή είναι αρκετά χρήσιμη για την προστασία από τους ιούς ηλεκτρονικού ταχυδρομείου οι οποίοι στέλνονται από εσωτερικούς χρήστες σε άλλους εσωτερικούς χρήστες επειδή αυτά τα μηνύματα δεν θα μπορούσαν να ανιχνευθούν από το φράγμα ασφάλειας. Προσφέρει πολύ καλύτερη ασφάλεια ενάντια μιας εσωτερικής «εξέγερσης» ενός ιού ηλεκτρονικού ταχυδρομείου.

Σχήμα 9-5: Υλοποίηση συστήματος ανίχνευσης ιών στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου

Το σημαντικότερο μειονέκτημα της εφαρμογής ανίχνευσης ιών στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου είναι η αρνητική επίπτωση στην απόδοσή του η οποία προκαλείται από την απαίτηση για ανίχνευση όλων των μηνυμάτων. Επίσης αρνητικό είναι και το γεγονός ότι η ανίχνευση ιών η οποία πραγματοποιείται στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου συχνά απαιτεί σημαντικές τροποποιήσεις στην υπάρχουσα διαμόρφωσή του. Παρ'όλα αυτά, η συγκεκριμένη επιλογή ανίχνευσης ιών παρέχει ορισμένα πλεονεκτήματα όπως:

- Το ηλεκτρονικό μήνυμα μπορεί να ανιχνευθεί και στις δυο κατευθύνσεις (εισερχόμενο και εξερχόμενο από το δίκτυο του οργανισμού).
- Δίδεται η δυνατότητα κεντρικής διαχείρισης της διαδικασίας ανίχνευσης των ηλεκτρονικών μηνυμάτων με στόχο να εξασφαλιστεί η συμμόρφωση με την πολιτική ασφάλειας του οργανισμού και η σωστή εφαρμογή και ενημέρωση του αντι-ιοικού λογισμικού.
- Προσφέρει προστασία στους εσωτερικούς χρήστες όταν ο ιός βρίσκεται στο εσωτερικό δίκτυο του οργανισμού.

Τα μειονεκτήματα αυτής της επιλογής είναι τα εξής:

- Η διαδικασία της ανίχνευσης μπορεί να απαιτήσει σημαντική τροποποίηση στη υπάρχουσα διαμόρφωση του εξυπηρετητή.
- Δεν μπορούν να ανιχνευθούν κρυπτογραφημένα μηνύματα.
- Απαιτούνται ισχυροί και ακριβοί εξυπηρετητές για να χειριστούν το φορτίο ενός μεγάλου οργανισμού.

Η ανίχνευση ιών η οποία είτε υλοποιείται σε φράγματα ασφάλειας είτε σε εξυπηρετητές ηλεκτρονικού ταχυδρομείου θα πρέπει να έχει τις ακόλουθες ιδιότητες:

- Ανιχνεύει και καθαρίζει όλους τους γνωστούς ιούς και άλλους τύπους «μοχθηρού κώδικα».
- Παρέχει προστασία από νέους και άγνωστους ιούς.
- Παρέχει φιλτράρισμα περιεχομένου.
- Παρέχει αυτοματοποιημένο «κατέβασμα» και εγκατάσταση των ενημερώσεων.
- Ενσωματώνει μηχανισμούς με σκοπό να αποτρέψει το ηλεκτρονικό ταχυδρομείο από την παράκαμψη του συστήματος.
- Παρέχει την αδυναμία/ανικανότητα στο ηλεκτρονικό ταχυδρομείο να παρακάμψει το σύστημα.
- Παρέχει την ευκολία στη διαχείριση.
- Παρέχει συχνές ενημερώσεις.
- Μπορεί να προσδιορίσει και να εφαρμόσει κανόνες σε διαφορετικούς τύπους περιεχομένου.
- Παρέχει έναν γερό και διαμορφώσιμο μηχανισμό προειδοποίησης.
- Παρέχει λεπτομερείς δυνατότητες καταγραφής.

Μια τρίτη επιλογή είναι η εγκατάσταση ανιχνευτών ιών στους υπολογιστές των πελατών (σχήμα 9-5). Αυτός ο τύπος ανιχνευτή ιών εγκαθίσταται στους τερματικούς σταθμούς των χρηστών. Τα ηλεκτρονικά μηνύματα ανιχνεύονται καθώς ανοίγονται από τους χρήστες. Το βασικό πλεονέκτημα αυτού του τύπου της διαμόρφωσης είναι ότι η ανίχνευση κατανέμεται μεταξύ πολλών υπολογιστών και επομένως έχει την ελάχιστη επίδραση στην απόδοση κάθε μεμονωμένου συστήματος. Η μέγιστη πρόκληση της εφαρμογής ανίχνευσης ιών στους τερματικούς σταθμούς των χρηστών είναι η δυσκολία στη διαχείριση των διανεμημένων ανιχνευτών ιών. Η κεντρική διαχείριση των διανεμημένων ανιχνευτών είναι αρκετά δύσκολη καθώς επίσης και η ενημέρωσή τους σε μια συνεχή βάση. Μια άλλη αδυναμία αυτής της επιλογής έγκειται στον βαθμό τον οποίο οι χρήστες ελέγχουν την λειτουργία του ανιχνευτή ιών καθώς πολλοί από αυτούς μπορούν να θέσουν εκτός λειτουργία μερικές ή όλες τις λειτουργίες του ανιχνευτή ιών, είτε τυχαία είτε σκόπιμα.

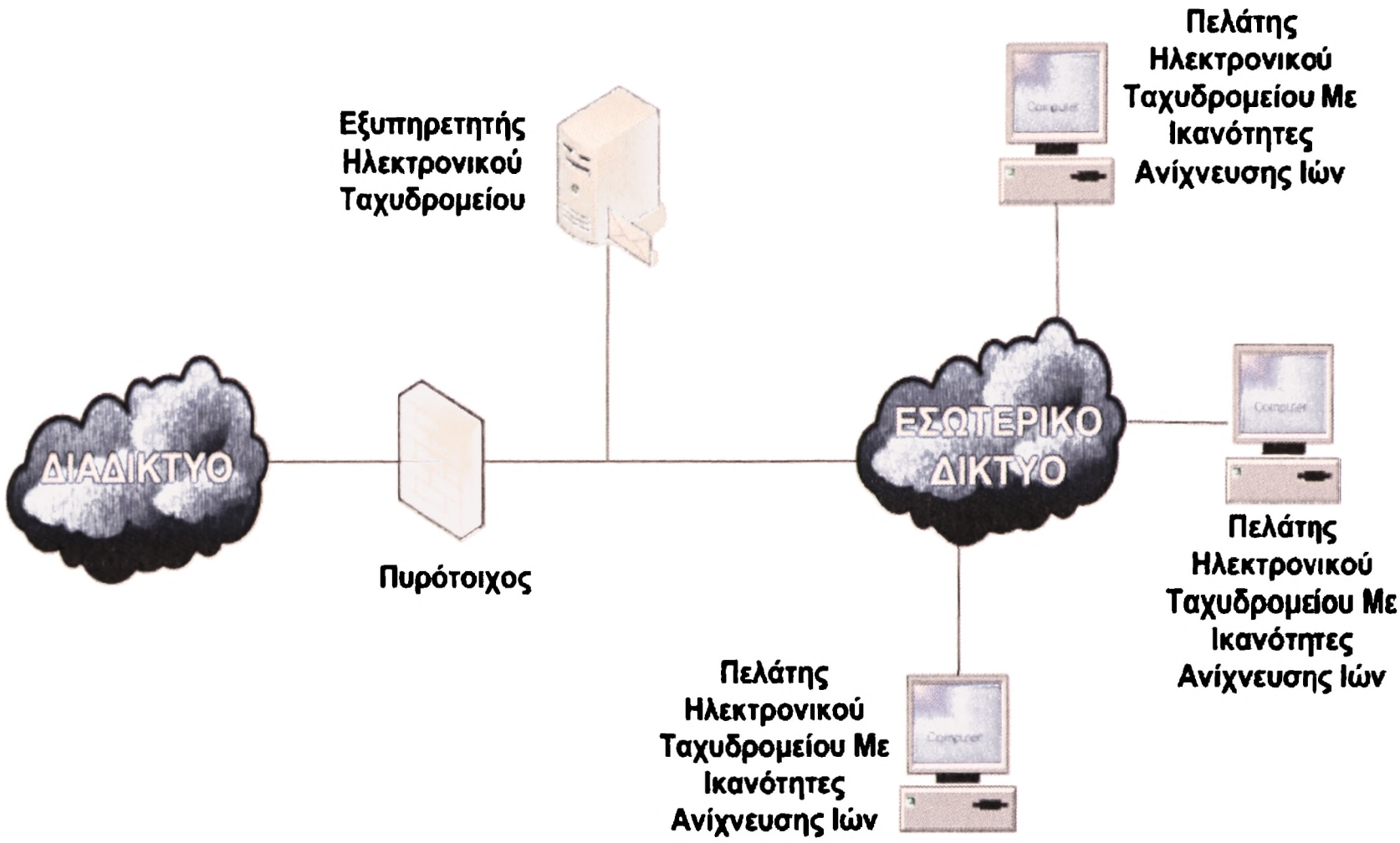
Τα πλεονεκτήματα της ανίχνευσης ιών στους τερματικούς σταθμούς των χρηστών είναι τα εξής:

- Δεν απαιτεί καμία τροποποίηση του εξυπηρετητή ηλεκτρονικού ταχυδρομείου.
- Μπορεί να ανιχνεύσει κρυπτογραφημένα μηνύματα όταν αυτά αποκρυπτογραφούνται από τον χρήστη.
- Διανέμει την ανίχνευση ιών και με αυτόν τον τρόπο ελαχιστοποιεί τον αντίκτυπο της ανίχνευσης σε οποιοδήποτε υπολογιστή.
- Προσφέρει προστασία στους εσωτερικούς χρήστες ακόμη και όταν ένας εσωτερικός χρήστης επιτρέψει την είσοδο ενός ιού (σκόπιμα ή άθελα).

Τα μειονεκτήματα της ανίχνευσης ιών στους τερματικούς σταθμούς των χρηστών είναι τα εξής:

- Δυσκολία στην κεντρική διαχείριση.
- Οι χρήστες μπορούν σκόπιμα ή τυχαία να θέσουν εκτός λειτουργίας ή να αποδυναμώσουν την προστασία που προσφέρεται από τον ανιχνευτή ιών.

- Ανιχνεύει μόνο τα εισερχόμενα μηνύματα.
- Οι χρήστες μπορεί να καθυστερούν να ενημερώνουν σε μια συνεχή βάση τον ανιχνευτή ιών με συνέπεια η οργάνωση να είναι πιο ευαίσθητη σε μια πιθανή «εξέγερση» ενός ιού.



Σχήμα 9-6: Υλοποίηση συστήματος ανίχνευσης ιών στους τερματικούς σταθμούς των χρηστών

Κάθε μια από τις παραπάνω επιλογές έχει τα πλεονεκτήματά της και τα μειονεκτήματά της, συνεπώς η υλοποίηση ανίχνευσης σε ένα μόνο σημείο (π.χ είτε στο φράγμα ασφάλειας είτε στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου είτε στα τερματικά των χρηστών) αφήνει αρκετά κενά ασφάλειας. Η ασφαλέστερη επιλογή είναι να εφαρμοστούν τουλάχιστον δυο επίπεδα ανίχνευσης ιών όπως π.χ η υλοποίηση ενός κεντρικού ανιχνευτή ιών (στο φράγμα ασφάλειας ή στον εξυπηρετητή) καθώς επίσης και ένα σύστημα ανίχνευσης ιών το οποίο θα προσφέρει ένα αρκετά ικανοποιητικό επίπεδο ασφάλειας στα τερματικά των τελικών χρηστών. Ωστόσο το σημαντικότερο βήμα είναι η συνεχής εκπαίδευση των χρηστών σε θέματα που αφορούν ιούς ηλεκτρονικού ταχυδρομείου και «μοχθηρό κώδικα».

Η συνεχής εκπαίδευση βοηθά τους χρήστες να κάνουν τις κατάλληλες ενέργειες, με σκοπό να αποφύγουν προβλήματα από ιούς και «μοχθηρό κώδικα», όπως:

- Να μην ανοίγουν ποτέ συνημμένα αρχεία από άγνωστους αποστολείς
- Να μην ανοίγουν ποτέ συνημμένα αρχεία με ύποπτες ή γνωστές ύποπτες επεκτάσεις αρχείων (π.χ attachment.txt.vbs, attachment.exe, κ.λ.π).
- Να είναι καχύποπτοι με μηνύματα από γνωστούς αποστολείς στα οποία η γραμμή αντικειμένου (subject line) ή το περιεχόμενο φαίνεται να είναι ανάρμοστο με την

υπάρχουσα σχέση (π.χ ένα μήνυμα με αντικείμενο "I LOVE YOU" από έναν επαγγελματικό συνάδελφο ή γενικά θέματα όπως "LOOK AT THIS, IT'S INTERESTING" κ.λ.π).

- Να ανιχνεύουν όλα τα συνημμένα αρχεία πριν τα ανοίξουν, κατά προτίμηση με διαμόρφωση του ανιχνευτή ιών να εκτελεί αυτόματα αυτή τη λειτουργία.
- Να ενημερώνουν την βάση δεδομένων του ανιχνευτή, σχετικά με καινούργια αρχεία υπογραφών ιών (viruses signature files), σε καθημερινή ή εβδομαδιαία βάση ή όταν συμβεί κάποιο «ξέσπασμα» ενός ιού.
- Βοηθά τους χρήστες να αναγνωρίσουν το ηλεκτρονικά μηνύματα που πιθανόν να κρύβουν κάποιον ιό με σκοπό να γίνουν οι κατάλληλες ενέργειες.

9.1.8 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Οι πολιτική ασφάλειας ηλεκτρονικού ταχυδρομείου που εφαρμόζει ένας οργανισμός εξαρτάται άμεσα από το επίπεδο επικινδυνότητας που τον χαρακτηρίζει. Ακολούθως αναφέρονται ορισμένα παραδείγματα πολιτικής ασφάλειας ηλεκτρονικού ταχυδρομείου ανάλογα με το επίπεδο επικινδυνότητας που χαρακτηρίζει έναν οργανισμό.

ΧΑΜΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Απαγορεύεται η χρήση υπηρεσιών ηλεκτρονικού ταχυδρομείου που αντίκεινται ή παρεμποδίζει τις λειτουργίες της επιχείρησης. Η επιχείρηση παρέχει στους εργαζομένους το ηλεκτρονικό ταχυδρομείο προκειμένου να εξυπηρετηθούν οι ανάγκες της επιχείρησης. Επιτρέπεται περιορισμένη προσωπική χρήση του ηλεκτρονικού ταχυδρομείου εφόσον δεν βλάπτονται τα συμφέροντα της επιχείρησης. Απαγορεύεται η χρήση του ηλεκτρονικού ταχυδρομείου για ιδιωτικούς εμπορικούς σκοπούς. Όλοι οι εργαζόμενοι θα πρέπει να έχουν λογαριασμό ηλεκτρονικού ταχυδρομείου. Επιτρέπεται η δημόσια πρόσβαση στους καταλόγους των ηλεκτρονικών διευθύνσεων της επιχείρησης. Εάν η επιχείρηση παρέχει δυνατότητα πρόσβασης στο ηλεκτρονικό ταχυδρομείο σε εξωτερικούς χρήστες τότε θα πρέπει οι εξωτερικοί χρήστες (σύμβουλοι, προσωρινοί υπάλληλοι ή συνεργάτες) του ηλεκτρονικού ταχυδρομείου της επιχείρησης να μελετήσουν και έπειτα να υπογράψουν την πολιτική ασφαλείας του ηλεκτρονικού ταχυδρομείου. Τα περιεχόμενα των ηλεκτρονικών μηνυμάτων αποτελούν εμπιστευτικές πληροφορίες της επιχείρησης και θα πρέπει να αποκαλύπτονται μόνο σε περίπτωση που διεξάγεται έρευνα.

ΜΕΣΑΙΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Η επιχείρηση παρέχει στους εργαζομένους το ηλεκτρονικό ταχυδρομείο προκειμένου να εξυπηρετηθούν οι ανάγκες της επιχείρησης. Δεν επιτρέπεται προσωπική χρήση του ηλεκτρονικού ταχυδρομείου. Εμπιστευτική ή ιδιωτική πληροφορία δεν θα πρέπει να αποστέλλεται μέσω του ηλεκτρονικού ταχυδρομείου. Θα πρέπει να χρησιμοποιείται μόνο εγκεκριμένο λογισμικό ηλεκτρονικού ταχυδρομείου. Οι χρήστες που παραβιάζουν την email πολιτική ασφαλείας θα πρέπει να υπόκεινται σε πειθαρχικές ποινές.

Το σύστημα ηλεκτρονικού ταχυδρομείου θα παρέχει μία μόνο δημόσια γνωστή ηλεκτρονική διεύθυνση για τους εργαζόμενους. Η ηλεκτρονική διεύθυνση δεν θα πρέπει να περιέχει ονόματα εσωτερικών συστημάτων ή ομάδων.

ΥΨΗΛΟ ΕΠΙΠΕΔΟ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Η επιχείρηση παρέχει στους εργαζομένους το ηλεκτρονικό ταχυδρομείο προκειμένου να εξυπηρετηθούν οι ανάγκες της επιχείρησης. Απαγορεύεται ρητά προσωπική χρήση του ηλεκτρονικού ταχυδρομείου. Όλα τα ηλεκτρονικά μηνύματα που δημιουργούνται ή αποθηκεύονται στους υπολογιστές ή στο δίκτυο της επιχείρησης αποτελούν περιουσιακό στοιχείο της επιχείρησης και δεν πρέπει να θεωρούνται ως ιδιωτικά. Για λόγους ασφαλείας η επιχείρηση διαθέτει το δικαίωμα να προσπελάσει τα ηλεκτρονικά μηνύματα των εργαζομένων. Τα περιεχόμενα των ηλεκτρονικών μηνυμάτων θα πρέπει να αποκαλύπτονται μόνο εάν αυτό επιβάλλεται από το νόμο ή για λόγους ασφαλείας. Οι χρήστες δεν θα πρέπει να επιτρέπουν σε τρίτους την αποστολή μηνυμάτων χρησιμοποιώντας το δικό τους λογαριασμό. Οι χρήστες δεν θα πρέπει να επιτρέπουν σε επιβλέποντες ή σε οποιοδήποτε συμβουλευτικό όργανο να χρησιμοποιήσει τον δικό τους λογαριασμό ηλεκτρονικού ταχυδρομείου. Δεν επιτρέπεται η δημόσια πρόσβαση στους καταλόγους των ηλεκτρονικών διευθύνσεων της επιχείρησης. Εάν μέσω του ηλεκτρονικού ταχυδρομείου αποστέλλεται εμπιστευτική πληροφορία της επιχείρησης τότε θα πρέπει να χρησιμοποιείται κρυπτογράφηση προκειμένου οι πληροφορίες που μεταφέρονται να είναι αναγνώσιμες μόνο από τον επιθυμητό παραλήπτη. Συνεργάτες ή προσωρινοί υπάλληλοι δεν θα πρέπει να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο της επιχείρησης. Η κρυπτογράφηση θα πρέπει να χρησιμοποιείται για κάθε πληροφορία που έχει αξιολογηθεί ως ευαίσθητη ή εμπιστευτική για την επιχείρηση προκειμένου να μεταδοθεί με ασφάλεια μέσω του ηλεκτρονικού ταχυδρομείου. Τα εξερχόμενα μηνύματα θα πρέπει να ελέγχονται προκείμενου να ελεχθεί εάν ακολουθείται η πολιτική ασφαλείας. Τα εισερχόμενα μηνύματα θα πρέπει να εξετάζονται για ιομορφικό λογισμικό. Οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου θα πρέπει να διαμορφωθούν έτσι ώστε να απορρίπτουν ηλεκτρονικά μηνύματα που δεν αποστέλλονται σε συστήματα της επιχείρησης. Τα αρχεία καταγραφής των εξυπηρετητών ηλεκτρονικού ταχυδρομείου πρέπει να εξετάζονται προκειμένου να εντοπιστεί η χρήση μη εγκεκριμένου λογισμικού ηλεκτρονικού ταχυδρομείου. Εάν εντοπιστεί η χρήση μη εγκεκριμένου λογισμικού ηλεκτρονικού ταχυδρομείου τότε θα πρέπει οι υπεύθυνοι χρήστες να αναφέρονται. Οι πελάτες ηλεκτρονικού ταχυδρομείου θα πρέπει να διαμορφωθούν έτσι ώστε κάθε μήνυμα που αποστέλλεται, να υπογράφεται ψηφιακά από τον αποστολέα.

ΚΕΦΑΛΑΙΟ 10ο

10.1 ΑΣΦΑΛΕΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

10.1 ΑΣΦΑΛΕΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Όταν κάποιος αναφέρεται στην ασφάλεια του Διαδικτύου, το πρώτο «αντίμετρο» που έρχεται στο μυαλό του είναι συνήθως η κρυπτογραφία. Αυτό οφείλεται στην αφύπνιση των καταναλωτών γενικά σε θέματα ασφάλειας και ειδικότερα σε ό,τι αφορά τους κινδύνους που δημιουργεί η μετάδοση αριθμών πιστωτικών καρτών ή/και τραπεζικών λογαριασμών μέσω του Διαδικτύου. Πέρα από τον όλο θόρυβο που έχει δημιουργηθεί, πραγματικά η κρυπτογραφία παίζει πολύ σημαντικό ρόλο στο Διαδίκτυο και ειδικότερα στον Παγκόσμιο Ιστό (World Wide Web-WWW). Συγκεκριμένα, επιτρέπει τη μετάδοση εμπιστευτικών πληροφοριών μέσα από ένα «μη ασφαλές» δίκτυο, χωρίς να υπάρχει κίνδυνος υποκλοπής ή ανεπιθύμητων παρεμβάσεων. Παράλληλα, επιτρέπει στις δύο πλευρές που επικοινωνούν να προβαίνουν σε αμοιβαία πιστοποίηση ταυτότητας.

Ένα πλήθος πρωτοκόλλων που χρησιμοποιούν κρυπτογραφία είναι διαθέσιμο στο Διαδίκτυο (Πίνακας 10-Α). Το κάθε ένα από αυτά χρησιμοποιείται για διαφορετικό σκοπό. Κάποια από αυτά έχουν σχεδιαστεί για την προστασία συγκεκριμένων υπηρεσιών, όπως είναι το *ηλεκτρονικό ταχυδρομείο* ή η *απομακρυσμένη πρόσβαση*.

Στον Παγκόσμιο Ιστό τα συνήθως χρησιμοποιούμενα πρωτόκολλα είναι (α) το SSL και (β) το SET. Το SSL (Secure Sockets Layer) είναι το κυρίαρχο πρωτόκολλο για την κρυπτογραφημένη επικοινωνία μεταξύ ενός προγράμματος πλοήγησης και ενός εξυπηρετητή διαδικτύου. Το SET (Secure Electronic Transactions) είναι ένα εξειδικευμένο πρωτόκολλο για την προστασία συναλλαγών μέσω πιστωτικών καρτών.

Πρωτόκολλο	Σκοπός
CyperCash	Ηλεκτρονικές τραπεζικές συναλλαγές
DNSSEC	Σύστημα ονοματολογίας πεδίων (DNS)
IPsec	Κρυπτογράφηση σε επίπεδο «πακέτου»
PCT	Κρυπτογράφηση σε επίπεδο TCP/IP
PGP	Ηλεκτρονικό ταχυδρομείο
S/MIME	Ηλεκτρονικό ταχυδρομείο
S-HTTP	Πλοήγηση στον παγκόσμιο Ιστό
Secure RPC	Απομακρυσμένες διαδικασίες κλήσης
SET	Ηλεκτρονικές τραπεζικές συναλλαγές
SSL	Κρυπτογράφηση σε επίπεδο TCP/IP
SSH	Απομακρυσμένη πρόσβαση
TLS	Κρυπτογράφηση σε επίπεδο TCP/IP

Πίνακας 10-Α: Πρωτόκολλα ασφαλείας που χρησιμοποιούνται στο Διαδίκτυο

10.1.1 SSL (Secure Socket Layer)

Το SSL (Secure Sockets Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου Ιστού, το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft. Το πρωτόκολλο SSL παρέχει *κρυπτογράφηση δεδομένων (data* encryption) *πιστοποίηση εξυπηρετητή* (server authentication), *ακεραιότητα μηνυμάτων* (message integrity) και *προαιρετική πιστοποίηση του πελάτη* (client authentication). Όσον αφορά το μήκος του *κλειδιού συνόδου* (session key) που δημιουργείται για κάθε κρυπτογραφημένη συναλλαγή, υπάρχουν δύο εκδόσεις του SSL: η έκδοση των 40 bits και αυτή των 128 bits. Φυσικά, όπως έχει ήδη αναφερθεί, όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογραφημένη επικοινωνία.

10.1.1.1 ΣΧΕΔΙΑΣΜΟΣ ΤΟΥ SSL

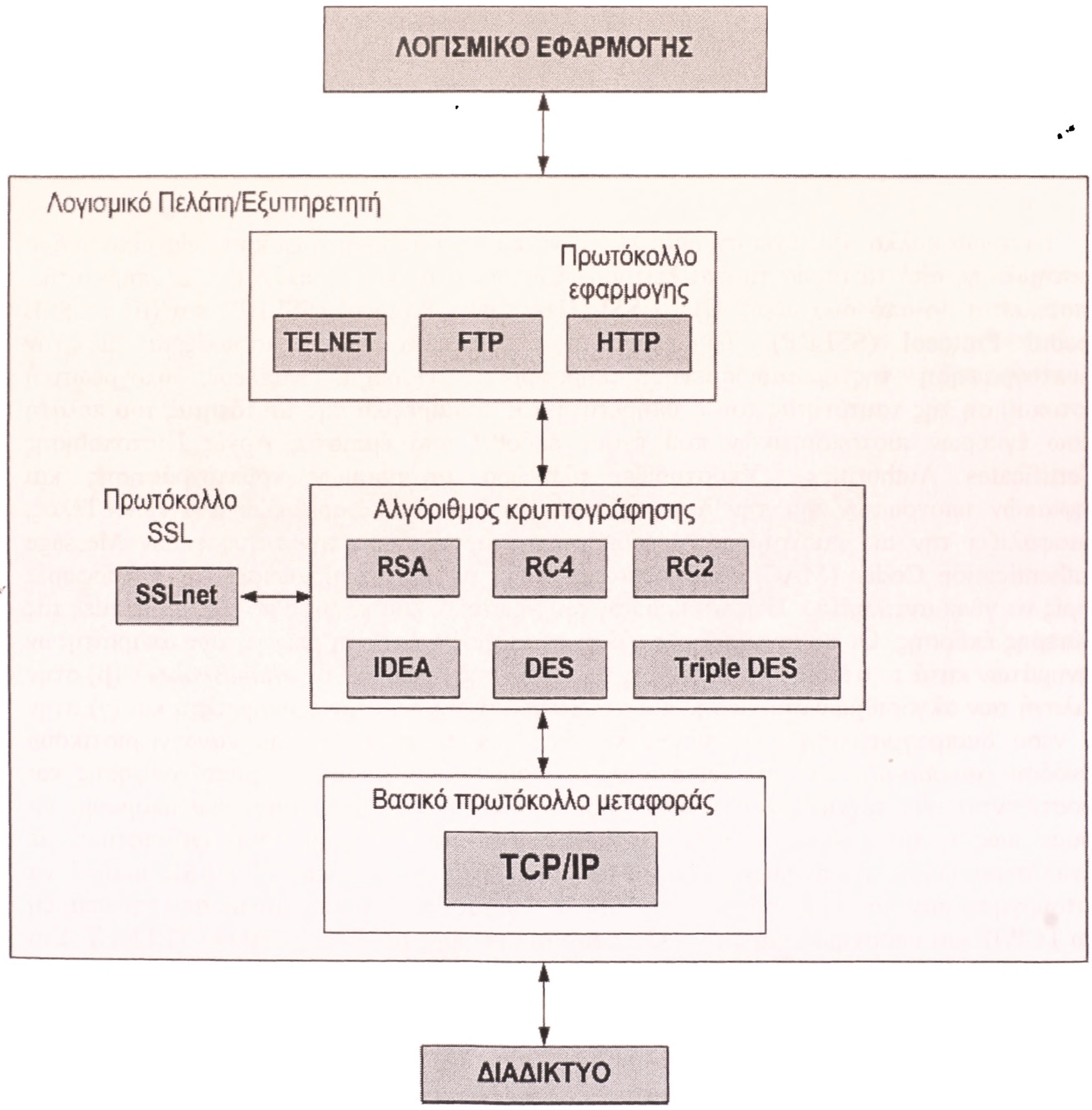
Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί ως πελάτης και το άλλο σαν εξυπηρετητής. Αποτελείται δε από δύο μέρη: (i) το SSL Handshake Protocol (SSLHP) και (ii) το SSL Record Protocol (SSLRP). Το απόρρητο της επικοινωνίας εξασφαλίζεται με την κρυπτογράφηση της μεταδιδόμενης πληροφορίας. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή και προαιρετικά της ταυτότητας του πελάτη μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μη μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Η τρίτη έκδοση του πρωτοκόλλου κάλυψε πολλές αδυναμίες της δεύτερης έκδοσης. Οι σημαντικότερες αλλαγές αφορούν: (α) στη μείωση των απαραίτητων μηνυμάτων κατά το στάδιο εγκαθίδρυσης της σύνδεσης («χειραψία», *«handshake»),* (β) στην επιλογή των αλγόριθμων συμπίεσης και κρυπτογράφησης από τον εξυπηρετητή και (γ) στην εκ νέου διαπραγμάτευση του κυρίως κλειδιού *(master-key)* και του «αναγνωριστικού» συνόδου *(session-id).* Ακόμη, αυξάνονται οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης και προστίθενται νέες τεχνικές για τη διαχείριση των κλειδιών. Συμπερασματικά μπορούμε να πούμε πως η τρίτη έκδοση (ν.3) του SSL είναι πιο ολοκληρωμένη σχεδιαστικά, με μεγαλύτερο εύρος υποστήριξης εφαρμογών και λιγότερες ατέλειες. Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Στο σχήμα 10-1 παρουσιάζεται διαγραμματικά η θέση του πρωτοκόλλου SSL στο λογισμικό μιας εφαρμογής.

10.1.1.2 ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Οι *αλγόριθμοι κρυπτογράφησης* που χρησιμοποιεί το πρωτόκολλο SSL χωρίζονται σε: (i) *αλγορίθμους ομάδας* (Block Ciphers) και (ii) *αλγορίθμους στοιχειοσειράς (*Stream Ciphers*).* Στα κρυπτογραφήματα στοιχειοσειράς ανήκουν οι RC4 με κλειδιά των 40 και 128 bits, ενώ

στα κρυπτογραφήματα ομάδας ανήκουν οι RC2 με κλειδιά 40 και 128 bits, οι DES, DES40 και άλλοι (Πίνακας 10-Β).

Οι αλγόριθμοι για την παραγωγή των τιμών κατακερματισμού (hash) και συγχώνευσης (digest) για τους κώδικες πιστοποίησης μηνύματος (Message Authentication Codes - MACs) είναι ο MD5 (Message Digest 5) (128-bit hash) και ο SHA (Secure Hash Algorithm) (160-bit hash). Η διαχείριση των κλειδιών γίνεται με ασύμμετρη κρυπτογραφία (RSA) και με το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman. Ο RSA μαζί με τον DSS και τον Fortezza μπορούν να χρησιμοποιηθούν για την ψηφιακή υπογραφή των κλειδιών κρυπτογράφησης.



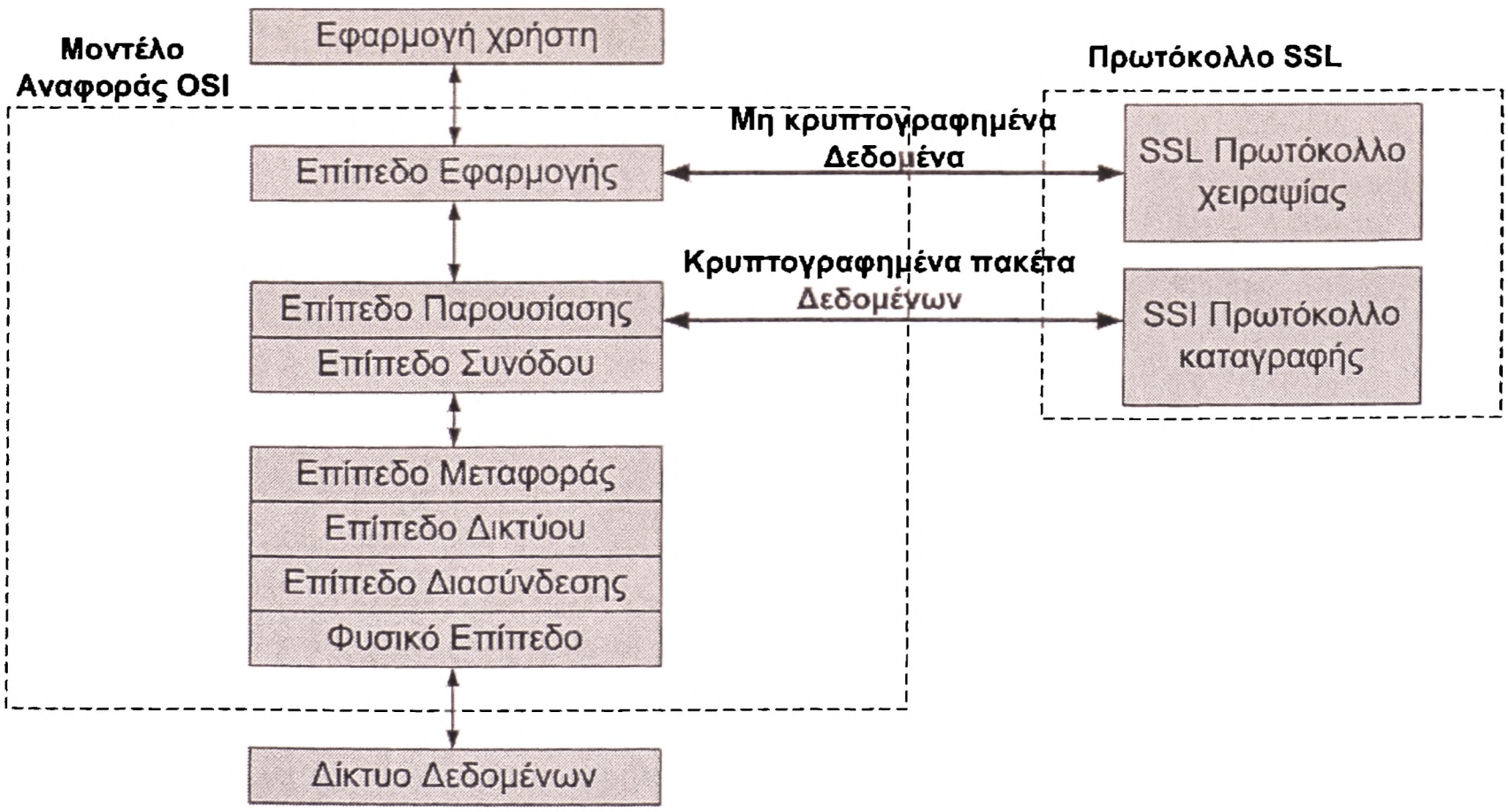
Σχήμα 10-1: Αναπαράσταση της θέσης του πρωτοκόλλου SSL στο λογισμικό μιας εφαρμογής

Αλγόριθμοι Ομάδας (Block Ciphers)		Αλγόριθμοι Στοιχειοσειράς (Stream Ciphers)	
Αλγόριθμος	**Μέγεθος κλειδιού**	**Αλγόριθμος**	**Μέγεθος κλειδιού**
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

Πίνακας 10-Β: Αλγόριθμοι κρυπτογράφησης του SSL (v.3)

10.1.1.3 ΤΟ SSL ΚΑΙ ΤΟ ΜΟΝΤΕΛΟ ΔΙΑΣΥΝΔΕΣΗΣ ΑΝΟΙΧΤΩΝ ΣΥΣΤΗΜΑΤΩΝ (OSI)

Στο Σχήμα 10-2 παρουσιάζεται η σχέση του πρωτοκόλλου SSL και του μοντέλου διασύνδεσης ανοικτών συστημάτων (OSI). Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο OSI, έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Από το σχήμα 10-2 παρατηρούμε πως το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επίσης είναι φανερό ότι η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL.

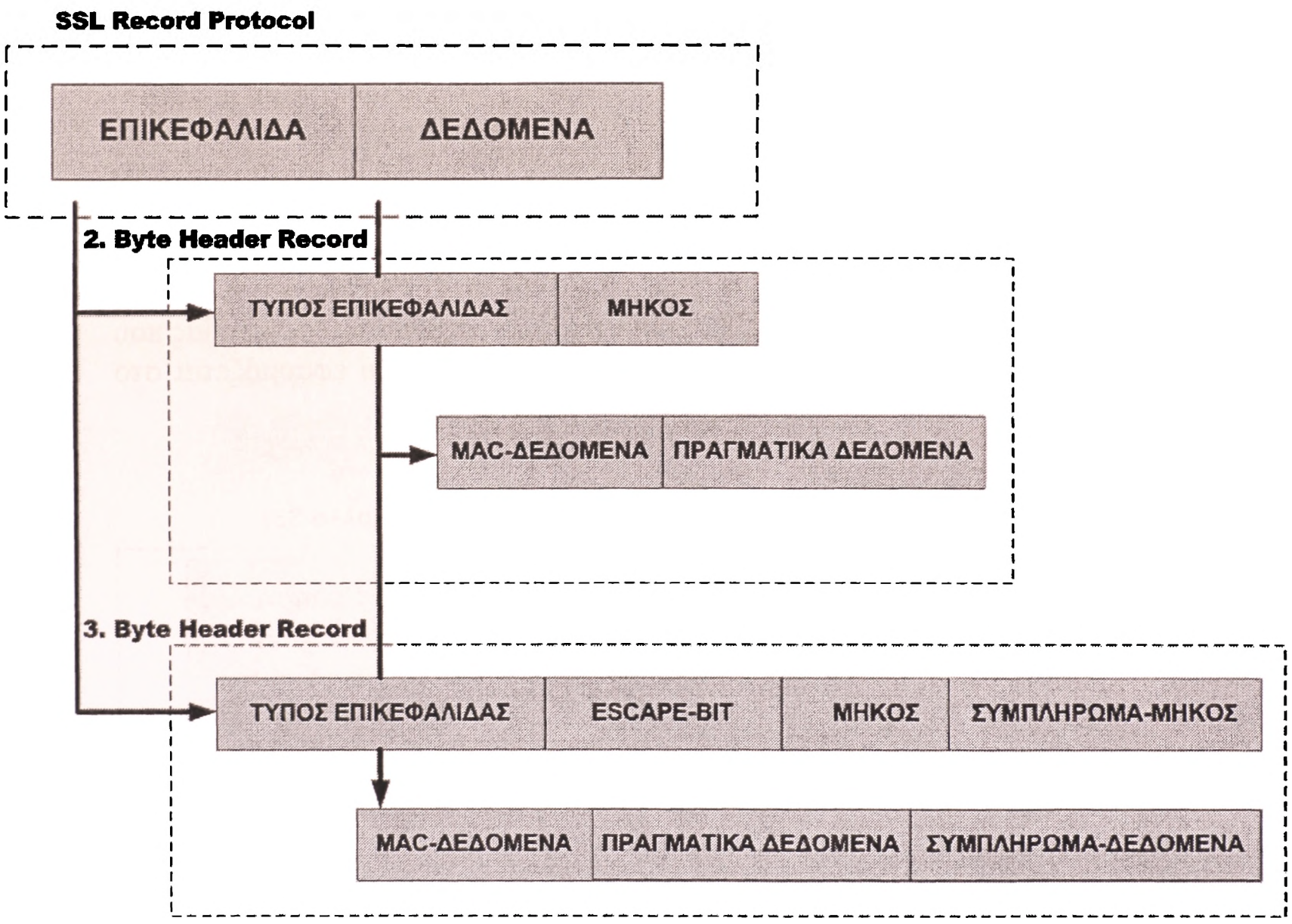


Σχήμα 10-2: Το SSL και το μοντέλο OSI

Παρατηρούμε επίσης ότι το SSL χωρίζεται σε δύο μέρη: (α) το SSL Handshake Protocol (SSLHP) και (β) το SSL Record Protocol (SSLRP). Το πρώτο διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του εξυπηρετητή και του πελάτη αν αυτό ζητηθεί. Το δεύτερο τοποθετεί τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει. Επίσης, εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα.

10.1.1.4 SSL Record Protocol (SSLRP)

Ένα πακέτο SSLRP αποτελείται από δύο μέρη: (α) την επικεφαλίδα και (β) τα δεδομένα. Η επικεφαλίδα μπορεί να έχει μήκος 2 ή 3 bytes. Είναι απαραίτητο να είναι 3 bytes όταν τα δεδομένα χρειάζονται συμπλήρωμα (padding). Το πεδίο escape-bit, στην περίπτωση των 3 bytes, προβλέπεται για ρύθμιση πληροφοριών εκτός ζώνης.



Σχήμα 10-3: Τρόπος λειτουργίας του SSL Record Protocol

Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes. Το κομμάτι των δεδομένων (data) αποτελείται από έναν Κώδικα Πιστοποίησης Μηνύματος (MAC-Message Authentication Code), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης (εάν αυτά χρειάζονται). Αυτό

το κομμάτι είναι που κρυπτογραφείται κατά τη μετάδοση. Τα συμπληρωματικά δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης είναι τύπου ομάδας και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα, ώστε το μέγεθος τους να είναι πολλαπλάσιο του μεγέθους που δέχεται σαν είσοδο το κρυπτογράφημα ομάδας. Εάν χρησιμοποιούνται αλγόριθμοι στοιχειοσειράς, τότε δεν απαιτείται συμπλήρωμα και μπορεί να χρησιμοποιηθεί η επικεφαλίδα των 2 bytes. Το MAC είναι η τιμή κατακερματισμού ή συγχώνευσης του ιδιωτικού κλειδιού του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας. Προβλέπεται και η *συμπίεση των δεδομένων (data compression)* με κατάλληλους μηχανισμούς που επιλέγονται κατά τη «χειραψία», ενώ δεν αποκλείεται να χρειαστεί και τεμαχισμός της πληροφορίας σε πολλά πακέτα (fragmentation).

10.1.1.5. ΠΡΩΤΟΚΟΛΛΟ «Χειραψίας» SSL (SSL Handshake protocol)

Το πρωτόκολλο χειραψίας SSL διαχωρίζεται σε δύο επιμέρους φάσεις: (α) Η πρώτη φάση αφορά στην επιλογή των αλγόριθμων, την ανταλλαγή ενός κύριου κλειδιού και την πιστοποίηση της ταυτότητας του εξυπηρετητή. (β) Η δεύτερη φάση υλοποιεί την πιστοποίηση της ταυτότητας του πελάτη (εάν ζητηθεί) και ολοκληρώνει την διαδικασία της «χειραψίας» (handshaking). Όταν ολοκληρωθούν και οι δύο φάσεις, το στάδιο της «χειραψίας» ολοκληρώνεται και αρχίζει η μεταφορά των δεδομένων. Όλα τα μηνύματα κατά τη διάρκεια της «χειραψίας» και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης *(Cipher Suite)* περιλαμβάνει: (α) τη μέθοδο για την ανταλλαγή των κλειδιών, (β) τον αλγόριθμο κρυπτογράφησης και (γ) το μηχανισμό για την παραγωγή του MAC.

Στη συνέχεια παρουσιάζονται τρεις διαφορετικές περιπτώσεις επικοινωνίας.

1. Πρώτα, εξετάζεται η περίπτωση της αρχικής σύνδεσης χωρίς πιστοποίηση ταυτότητας του πελάτη. Χρησιμοποιείται ο συμβολισμός ***"{data}key"*** για να υποδηλώσει δεδομένα που είναι κρυπτογραφημένα με το κλειδί ***"key"***. Η ακολουθία μηνυμάτων (βήμα-προς-βήμα) φαίνεται στον Πίνακα 10-Γ (όπου C-Client και όπου S-Server).

Με το μήνυμα ***client-hello*** ο πελάτης (client) στέλνει στον εξυπηρετητή μια λίστα με τους αλγόριθμους που υποστηρίζει και τα δεδομένα πρόκλησης (challenge-data) που θα χρησιμοποιηθούν αργότερα για την πιστοποίηση της ταυτότητας του. Το μήνυμα ***server-hello*** επιστρέφει στον πελάτη ένα αναγνωριστικό της σύνδεσης ***(connection-id),*** την επιλογή του εξυπηρετητή όσον αναφορά το πακέτο των αλγόριθμων κρυπτογράφησης και συμπίεσης (που και οι δύο υποστηρίζουν) και το πιστοποιητικό του εξυπηρετητή που θα χρησιμοποιηθεί από τον πελάτη για την απόκτηση του δημοσίου κλειδιού του εξυπηρετητή.

Από αυτό το σημείο και μετά όλα τα μηνύματα κρυπτογραφούνται στο επίπεδο του πρωτοκόλλου SSL Record. Το ***master-key*** δε χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγαριών κλειδιών. Το ένα ζευγάρι ανήκει στον πελάτη και αποτελείται από το ***client-write-key*** που χρησιμοποιεί ο πελάτης για να κρυπτογραφήσει τα μηνύματα προς τον εξυπηρετητή και το ***client-read-key*** για να αποκρυπτογραφήσει ό,τι λαμβάνει από αυτόν. Το δεύτερο ζευγάρι ανήκει στον εξυπηρετητή και αποτελείται από το ***server-write-key*** για κρυπτογράφηση μηνυμάτων προς τον πελάτη και το ***server-read-key*** για αποκρυπτογράφηση των λαμβανομένων. Αξίζει να σημειωθεί ότι το ***client-write-key*** είναι το ίδιο με το ***server-read-key*** και το ***client-read-key*** είναι το ίδιο με το ***server-write-key.***

Το ***client-finish*** περιέχει το αναγνωριστικό της σύνδεσης που αρχικά είχε σταλεί από τον εξυπηρετητή κρυπτογραφημένο με το ***client-write-key.***

Το ***server-verify*** περιέχει τα ***challenge-data*** που είχε στείλει ο πελάτης στον εξυπηρετητή κατά την αρχή της σύνδεσης, κρυπτογραφημένα με το ***server-write-key.*** Η παραλαβή και αποκρυπτογράφηση αυτού του μηνύματος είναι το τελικό στάδιο για την επιβεβαίωση της ταυτότητας του εξυπηρετητή αφού μόνο ο αληθινός εξυπηρετητής θα μπορούσε να αποκρυπτογραφήσει το ***master-key*** με το ιδιωτικό του κλειδί.

Τέλος, το μήνυμα ***server-finish*** τερματίζει τη «χειραψία». Περιέχει το αναγνωριστικό συνόδου ***(session-id)*** που χρησιμοποιείται σε επόμενες διαδικασίες «χειραψίας» για την αποφυγή επανάληψης της φάσης επιλογής αλγορίθμων και ανταλλαγής του ***master-key***. Το ***session-id*** αποθηκεύεται και από τους δύο και η προτεινόμενη διάρκεια ζωής είναι 100 δευτερόλεπτα. Έπειτα, καταργείται.

Τύπος μηνύματος	Κατεύθυνση	Δεδομένα που μεταφέρονται
Client-hello	C⇨S	Challenge-data, cipher-suite-specs, compressions
Server-hello	C⇦S	Connection-id, server-certificate, cipher-kind, Compression-kind
Client-master-key	C⇨S	Clear-master-key,{secret-master-key}server public Key
Client-finish	C⇨S	{connection-id}client-write-key
Server-verify	C⇦S	{challenge-data}server-write-key
Server-finish	C⇦S	{session-id}server-write-key

Πίνακας 10-Γ

2. Όταν ένα προηγούμενο ***session-id*** του πελάτη χρησιμοποιείται για να επανεγκαταστήσει τη σύνδεση, η «χειραψία» γίνεται όπως φαίνεται στον παρακάτω πίνακα (πίνακας 10-Δ):

Τύπος μηνύματος	Κατεύθυνση	Δεδομένα που μεταφέρονται
Client-hello	C⇨S	Challenge-data, session-id, cipher-suite-specs, compressions
Server-hello	C⇦S	Connection-id
Client-finish	C⇨S	{connection-id}client-write-key
Server-verify	C⇦S	{challenge-data}server-write-key
Server-finish	C⇦S	{session-id}server-write-key

Πίνακας 10-Δ

Αλλάζει το ***client-hello*** που περιέχει επιπλέον το ***session-id*** και χρησιμοποιείται από τον εξυπηρετητή για να καθορίσει τους αλγόριθμους και το ***master-key***. Η λίστα με τους αλγόριθμους αποστέλλεται ξανά για την περίπτωση κατά την οποία έχει λήξει το ***session-id.*** Το ***server-hello*** αποστέλλεται μόνο όταν το ***session-id*** ισχύει ακόμα.

3. Όταν ζητείται πιστοποίηση της ταυτότητας του πελάτη και έχει προηγουμένως εκδοθεί ***session-id***, η ακολουθία των μηνυμάτων της «χειραψίας» γίνεται όπως φαίνεται στον ακόλουθο πίνακα (πίνακας 10-Ε):

Τύπος μηνύματος	Κατεύθυνση	Δεδομένα που μεταφέρονται
Client-hello	C⇨S	Challenge-data, session-id, cipher-suite-specs
Server-hello	C⇦S	Connection-id, server-certificate, cipher-kind
Client-master-key	C⇨S	Clear-master-key,{secret-master-key}server public Key
Client-finish	C⇨S	{connection-id}client-write-key
Server-verify	C⇦S	{challenge-data}server-write-key
Request-certificate	C⇦S	{auth-type, cert-chal-data}server-write-key
Client-certificate	C⇨S	{cert-type, client-cert, resp-data}client-write-key
Server-finish	C⇦S	{session-id}server-write-key

Πίνακας 10-Ε

Παρατηρούμε ότι προστέθηκαν δύο νέα μηνύματα στην ακολουθία που παρουσιάστηκε προηγουμένως. Το ***request-certificate*** στέλνεται από τον εξυπηρετητή και περιέχει μια δήλωση για τη συνάρτηση που θα χρησιμοποιήσει ο πελάτης για την παραγωγή της τιμής συγχωνεύσεως μηνύματος και τον τύπο της συμμετρικής κρυπτογράφησης. Επίσης, αποστέλλονται και δεδομένα που θα υπογράψει ο πελάτης για να αποδείξει την ταυτότητα του ***(cert-chal-data).***

Το *client-certificate* επιστρέφει στον εξυπηρετητή το πιστοποιητικό του πελάτη, μαζί με μια δήλωση του τύπου αυτού ***(cert-type)*** και την υπογραφή των δεδομένων ***cert-chal-data.*** Ο εξυπηρετητής θα χρησιμοποιήσει το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό του πελάτη για να αποκρυπτογραφήσει την υπογραφή. Έπειτα, θα υπολογίσει τη συγχώνευση μηνύματος (message digest) των ***cert-chal-data*** και θα το συγκρίνει με τη συγχώνευση μηνύματος που προήλθε από την αποκρυπτογράφηση της υπογραφής.

Κατά την διάρκεια όλων των παραπάνω ανταλλαγών μηνυμάτων, μηνύματα λάθους μπορούν να σταλούν ως απάντηση σε μηνύματα «άνευ νοήματος». Η διαδικασία αναγνώρισης λάθους και η αποστολή του κατάλληλου μηνύματος αναλαμβάνεται από το πρωτόκολλο SSL Alert Protocol που αποτελεί μέρος του SSL Handshake Protocol. Έτσι, το μήνυμα ***no-cipher-error*** στέλνεται όταν ο εξυπηρετητής δεν υποστηρίζει κανένα από τους αλγόριθμους που προτείνει ο πελάτης, το μήνυμα ***no-certificate-error*** όταν δεν είναι διαθέσιμο το ζητούμενο πιστοποιητικό, το μήνυμα ***bad-certificate*** αν το πιστοποιητικό είναι άκυρο και τέλος το ***unsupported-certificate-type-error,*** όταν ο τύπος ενός πιστοποιητικού δεν υποστηρίζεται από κανέναν.

10.1.2 SET (Secure Electronic Transactions)

Το SET (Secure Electronic Transactions) είναι ένα πρωτόκολλο κρυπτογράφησης που αναπτύχθηκε από κοινού από τη Visa, τη MasterCard, τη Netscape και τη Microsoft.

Αντίθετα με το SSL το οποίο είναι ένα σύστημα γενικού σκοπού για κρυπτογραφημένη επικοινωνία, το SET είναι πολύ εξειδικευμένο. Χρησιμοποιείται *μόνο* για την ασφαλή συναλλαγή μέσω πιστωτικών καρτών και επιταγών ανάμεσα στους πελάτες και τους εμπόρους. Σε χαμηλό επίπεδο, το πρωτόκολλο SET παρέχει τις ακόλουθες βασικές υπηρεσίες [Stall99]:

- **Πιστοποίηση:** Όλα τα μέλη που συμμετέχουν σε μία συναλλαγή μέσω πιστωτικής κάρτας πιστοποιούνται χρησιμοποιώντας ψηφιακές υπογραφές. Αυτό περιλαμβάνει τους πελάτες, τον έμπορο, την τράπεζα που εκδίδει την πιστωτική κάρτα του πελάτη και την τράπεζα που διαχειρίζεται το λογαριασμό του εμπόρου.
- **Εμπιστευτικότητα:** Η συναλλαγή είναι κρυπτογραφημένη έτσι ώστε να μη μπορεί να υποκλαπεί.
- **Ακεραιότητα του μηνύματος:** Κανένας δε μπορεί να επέμβει στη συναλλαγή με σκοπό να μεταβάλλει τον αριθμό λογαριασμού ή το ποσό της συναλλαγής.
- **Διασύνδεση:** Το SET επιτρέπει σε ένά μήνυμα που στέλνεται σε ένα μέλος να περιέχει μια προσάρτηση (attachment) που μπορεί. να διαβαστεί μόνο από ένα άλλο μέλος. Η διασύνδεση επιτρέπει στο πρώτο μέλος να επιβεβαιώσει ότι η προσάρτηση είναι σωστή χωρίς να είναι σε θέση να διαβάσει τα περιεχόμενα αυτής.

Σε υψηλό επίπεδο, το πρωτόκολλο SET υποστηρίζει σε πραγματικό χρόνο όλες τις δυνατότητες του υπάρχοντος συστήματος πιστωτικών καρτών, συμπεριλαμβανομένων των ακολούθων:

- Εγγραφή κατόχου πιστωτικής κάρτας.
- Εγγραφή εμπόρου.
- Αιτήσεις αγοράς.
- Πιστοποιήσεις πληρωμής.
- Μεταφορά διαθέσιμων χρηματικών πόρων.
- Επιστροφές αμφισβητούμενων χρεώσεων.
- Πιστώσεις.
- Συναλλαγές μέσω επιταγών

Οι βασικοί συμμετέχοντες στο περιβάλλον του SET είναι:

- **Ο εκδότης:** Ένας οικονομικός οργανισμός που εκδίδει τραπεζικές κάρτες (πιστωτικές ή ανάληψης χρημάτων).

- **Ο κάτοχος:** Ένας εξουσιοδοτημένος κάτοχος μιας τραπεζικής κάρτας ο οποίος είναι σε θέση, με την άδεια του εκδότη, να εκτελεί αγορές ηλεκτρονικού εμπορίου.

- **Ο πωλητής:** Κάποιος που πουλάει αγαθά, υπηρεσίες ή πληροφορίες και δέχεται πληρωμές ηλεκτρονικά.

- **Ο οργανισμός:** Κάποιο οικονομικό-πιστωτικό ίδρυμα που υποστηρίζει τους πωλητές παρέχοντας υπηρεσίες για την επεξεργασία συναλλαγών με τραπεζικές κάρτες.

Δευτερεύοντες συμμετέχοντες που όμως αποτελούν μέρος της όλης δομής του πρωτοκόλλου SET είναι:

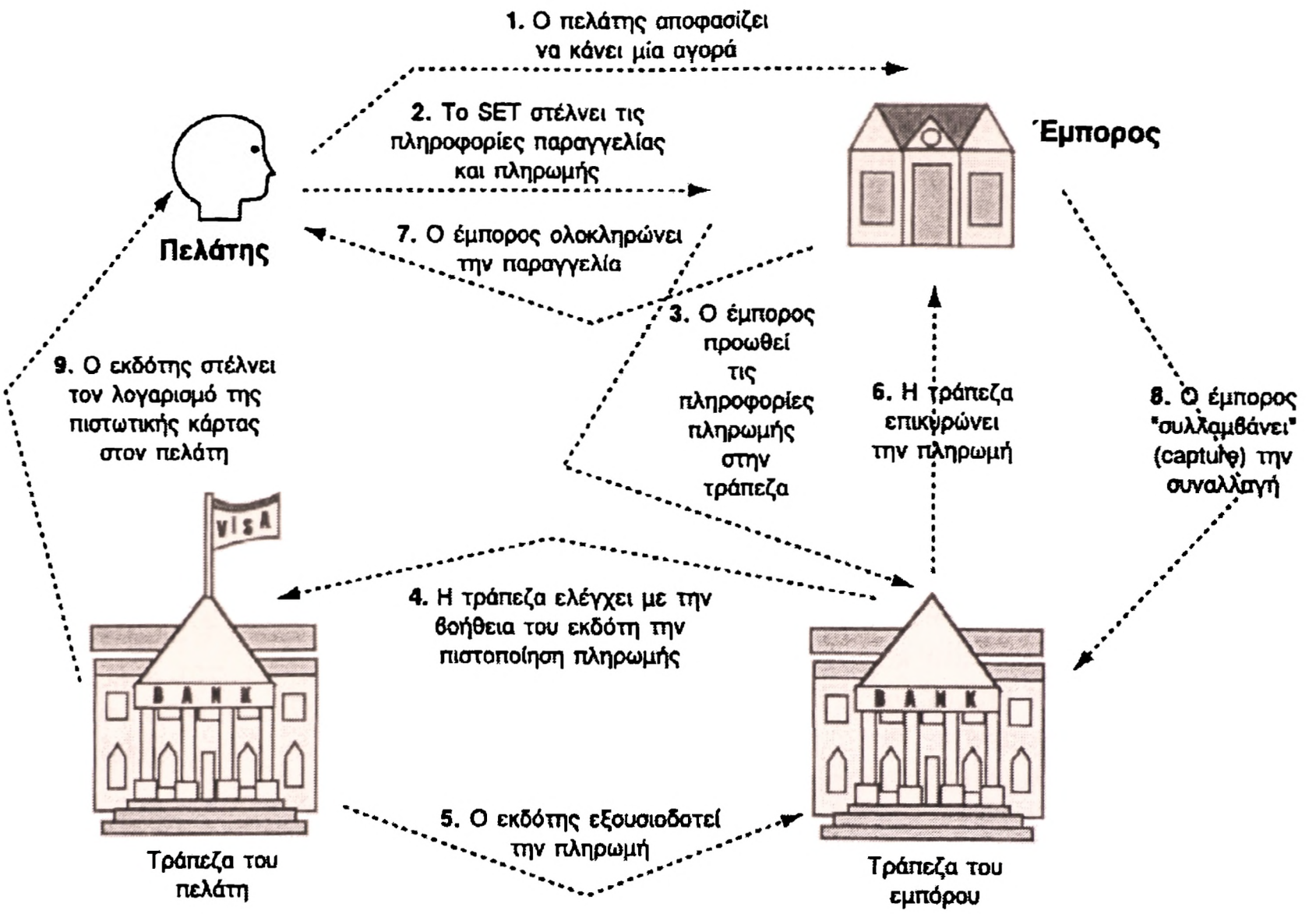
- **Η πύλη πληρωμής:** Ένα σύστημα που παρέχει ηλεκτρονικές υπηρεσίες εμπορίου σε πραγματικό χρόνο (online) στους πωλητές. Ένα τέτοιο σύστημα το διαχειρίζεται κάποιος οργανισμός.
- **Οι αρχές πιστοποίησης:** Συστατικά της όλης δομής που πιστοποιούν τα δημόσια κλειδιά των κατόχων, των πωλητών και των οργανισμών (με τις αντίστοιχες πύλες τους).

10.1.2.1 Η ΣΥΝΑΛΛΑΓΗ SET

Στο πρωτόκολλο SET εμπλέκονται τέσσερις φορείς: (1) Ο κάτοχος της κάρτας, (2) ο έμπορος, (3) η τράπεζα που εκδίδει την πιστωτική κάρτα και (4) η τράπεζα του εμπόρου. Όπως και με τα άλλα πρωτόκολλα κρυπτογράφησης, το SET χρησιμοποιεί ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού και υπογεγραμμένα πιστοποιητικά ταυτότητας στα μέλη που παίρνουν μέρος στην συναλλαγή και για να τους επιτρέψει να ανταλλάξουν μηνύματα εμπιστευτικού περιεχομένου. Κατά τη διάρκεια μίας συναλλαγής πώλησης ενός προϊόντος, το πρωτόκολλο SET λειτουργεί ως εξής (Σχήμα 10-4).

1. **Ο πελάτης ξεκινά μία αγορά:** Ο πελάτης που βρίσκεται στον εμπορικό δικτυακό τόπο της αρεσκείας του αποφασίζει ότι θέλει να αγοράσει κάποιο προϊόν και συμπληρώνει μια φόρμα παραγγελίας που περιλαμβάνει την περιγραφή του εμπορεύματος και πληροφορίες αποστολής. Αυτό είναι και το μόνο που χρειάζεται πριν ξεκινήσει τη λειτουργία του το πρωτόκολλο SET, χρησιμοποιώντας CGI scripts ή κάποιο άλλο κατάλληλο λογισμικό. Η λειτουργία του πρωτοκόλλου SET ξεκινά μόλις ο χρήστης πατήσει το «κουμπί» πληρωμής. Ο εξυπηρετητής τώρα στέλνει στον υπολογιστή του πελάτη ένα μήνυμα ότι ξεκινά το λογισμικό SET μέσω ενός εγγράφου με ειδικό τύπο MIME, μέσω ενός ActiveX control, ή μέσω ενός Java applet.

2. **Το λογισμικό του πελάτη στέλνει τις πληροφορίες παραγγελίας και πληρωμής:** Το λογισμικό SET του πελάτη δημιουργεί δύο μηνύματα. Το πρώτο μήνυμα περιέχει πληροφορίες παραγγελίας που αποτελούνται από τη συνολική τιμή αγοράς και τον αριθμό παραγγελίας. Το δεύτερο μήνυμα περιέχει πληροφορίες πληρωμής που αποτελούνται από τον αριθμό της πιστωτικής κάρτας του πελάτη και πληροφορίες της τράπεζας. Οι πληροφορίες παραγγελίας είναι κρυπτογραφημένες χρησιμοποιώντας ένα τυχαίο συμμετρικό κλειδί συνόδου και «πακεταρισμένες» σε ένα ψηφιακό φάκελο χρησιμοποιώντας το δημόσιο κλειδί του εμπόρου. Οι πληροφορίες πληρωμής είναι ομοίως κρυπτογραφημένες, αλλά αυτή τη φορά χρησιμοποιώντας το δημόσιο κλειδί της τράπεζας του εμπόρου. Αυτό εμποδίζει τον έμπορο από το να «δει» τον αριθμό της πιστωτικής κάρτας ή την τράπεζα από το να "δει" τις πληροφορίες παραγγελίας. Το λογισμικό τώρα υπολογίζει μια συνάρτηση κατακερματισμού (hash) των πληροφοριών παραγγελίας και πληρωμής και το υπογράφει με το ιδιωτικό κλειδί του πελάτη. Αυτό δημιουργεί μία «διπλή υπογραφή» (dual signature) που επιτρέπει και στον έμπορο και στην τράπεζα του να ελέγξουν την ακεραιότητα και των δύο μηνυμάτων χωρίς να είναι σε θέση να διαβάσουν τα περιεχόμενα που έχουν.



Σχήμα 10-4: Η συναλλαγή SET

3. **Ο έμπορος στέλνει τις πληροφορίες πληρωμής στην τράπεζα:** Το λογισμικό SET του εμπορικού εξυπηρετητή Web δημιουργεί μία αίτηση εξουσιοδότησης, προωθώντας τις πληροφορίες πληρωμής του πελάτη σε έναν εξυπηρετητή SET που διατηρείται από την τράπεζα του εμπόρου. Ο έμπορος υπογράφει την αίτηση εξουσιοδότησης με το ιδιωτικό του κλειδί, με σκοπό να πιστοποιήσει την ταυτότητα του στην τράπεζα. Η αίτηση αυτή είναι κρυπτογραφημένη με ένα νέο τυχαίο κλειδί συνόδου και ενσωματωμένη μέσα σε ένα ψηφιακό φάκελο χρησιμοποιώντας το δημόσιο κλειδί της τράπεζας.

4. **Η τράπεζα ελέγχει την εγκυρότητα της κάρτας:** Η τράπεζα αποκρυπτογραφεί την αίτηση εξουσιοδότησης του εμπόρου και επαληθεύει την ταυτότητα του εμπόρου. Μετά αποκρυπτογραφεί τις πληροφορίες πληρωμής του πελάτη και επαληθεύει την ταυτότητα του πελάτη. Στη συνέχεια, δημιουργεί τη δική της αίτηση εξουσιοδότησης, την υπογράφει και την προωθεί στον εκδότη της πιστωτικής κάρτας.

5. **Ο Εκδότης της κάρτας εξουσιοδοτεί και υπογράφει την αίτηση:** Η τράπεζα του πελάτη επιβεβαιώνει την ταυτότητα της τράπεζας του εμπόρου, αποκρυπτογραφεί τις πληροφορίες και ελέγχει τον τραπεζικό λογαριασμό του πελάτη. Εάν ο τραπεζικός λογαριασμός είναι έγκυρος, ο εκδότης της πιστωτικής κάρτας εγκρίνει την αίτηση εξουσιοδότησης υπογράφοντας την και επιστρέφοντας την στην τράπεζα του εμπόρου.

6. **Η τράπεζα του εμπόρου επικυρώνει τη συναλλαγή:** Η τράπεζα του εμπόρου τώρα επικυρώνει τη συναλλαγή κα; την υπογράφει, στέλνοντας το OK πίσω στον εμπορικό εξυπηρετητή διαδικτύου.

7. **Ο εμπορικός διαδικτυακός εξυπηρετητής ολοκληρώνει τη συναλλαγή:** Ο εμπορικός διαδικτυακός εξυπηρετητής αναγνωρίζει ότι η κάρτα εγκρίθηκε δείχνοντας στον πελάτη μία σελίδα επιβεβαίωσης και στη συνέχεια εισάγει την παραγγελία στο σύστημα επεξεργασίας των παραγγελιών του εμπόρου. Ύστερα από κάποιο χρονικό διάστημα, ο έμπορος στέλνει το εμπόρευμα στον πελάτη του.

8. **Ο έμπορος "συλλαμβάνει" (capture) τη συναλλαγή:** Στην τελική φάση μίας τυπικής SET αλληλεπίδρασης, ο έμπορος στέλνει ένα μήνυμα «σύλληψης» (capture) στην τράπεζα του. Αυτό επιβεβαιώνει την αγορά και προκαλεί τη χρέωση της πιστωτικής κάρτας του πελάτη. Ο τραπεζικός λογαριασμός του εμπόρου θα πιστωθεί.

9. **Ο εκδότης της πιστωτικής κάρτας στέλνει το λογαριασμό στον πελάτη:** Η χρέωση εμφανίζεται στη μηνιαία κατάσταση λογαριασμού του πελάτη μαζί με άλλες ίσως χρεώσεις.

Υπάρχουν βήματα πιστοποίησης σε κάθε φάση του πρωτοκόλλου SET. Αυτό είναι σημαντικό, ώστε να αποτραπεί τυχόν παρακολούθηση της συναλλαγής από κάποιον «κακόβουλο». Για να το επιτύχει αυτό, το SET χρησιμοποιεί μία ιεραρχία αξιοπιστίας. Μια αξιόπιστη "εξουσία πιστοποίησης" θα δημιουργήσει πιστοποιητικά X.5O9v3 [RFC 3280] και για τον εκδότη της πιστωτικής κάρτας και για την τράπεζα του εμπόρου. Πριν ο έμπορος ή ο κάτοχος της κάρτας χρησιμοποιήσει το σύστημα SET, πρέπει πρώτα να εγγραφεί. Όταν ένας πελάτης εγγράφει ηλεκτρονικά την πιστωτική του κάρτα με το σύστημα SET, το λογισμικό SET δημιουργεί ένα ζεύγος κλειδιών αποτελούμενο από ένα δημόσιο και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί υπογράφεται από τον εκδότη της τράπεζας και επιστρέφεται στον πελάτη ως ένα υπογεγραμμένο πιστοποιητικό X.5O9v3. Παρόμοια, η τράπεζα του εμπόρου δίνει στον έμπορο ένα πιστοποιητικό όταν ανοίγει έναν λογαριασμό για να δεχθεί τις πληρωμές μέσω πιστωτικών καρτών.

Σε αντίθεση με το πρωτόκολλο SSL που χρησιμοποιεί το ίδιο ζεύγος κλειδιών και για την κρυπτογράφηση και για τις ψηφιακές υπογραφές, το πρωτόκολλο SET χρησιμοποιεί δύο ζεύγη κλειδιών. Ο έμπορος, η τράπεζα του εμπόρου και η τράπεζα που εκδίδει την πιστωτική κάρτα του πελάτη έχουν όλοι δύο ζεύγη κλειδιών. Το ένα χρησιμοποιείται για την κρυπτογράφηση και το άλλο χρησιμοποιείται για τις ψηφιακές υπογραφές.

Τεχνικά, το πρωτόκολλο SET χρησιμοποιεί το αλγόριθμο κατακερματισμού SHA (Secure Hash Algorithm), ο οποίος παράγει έναν αριθμό των 160 bits. Το ζεύγος κλειδιών χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RSA και τα κλειδιά έχουν μήκος 1.024 bits. Αν και το SET μπορεί να χρησιμοποιήσει διαφόρους αλγορίθμους για συμμετρική κρυπτογράφηση, χρησιμοποιεί συνήθως τον DBS, το κλειδί του.

ΠΑΡΑΡΤΗΜΑ Α

ΕΙΚΟΝΕΣ ΙΩΝ ΔΙΑΔΙΚΤΥΟΥ VIRUS IMAGES

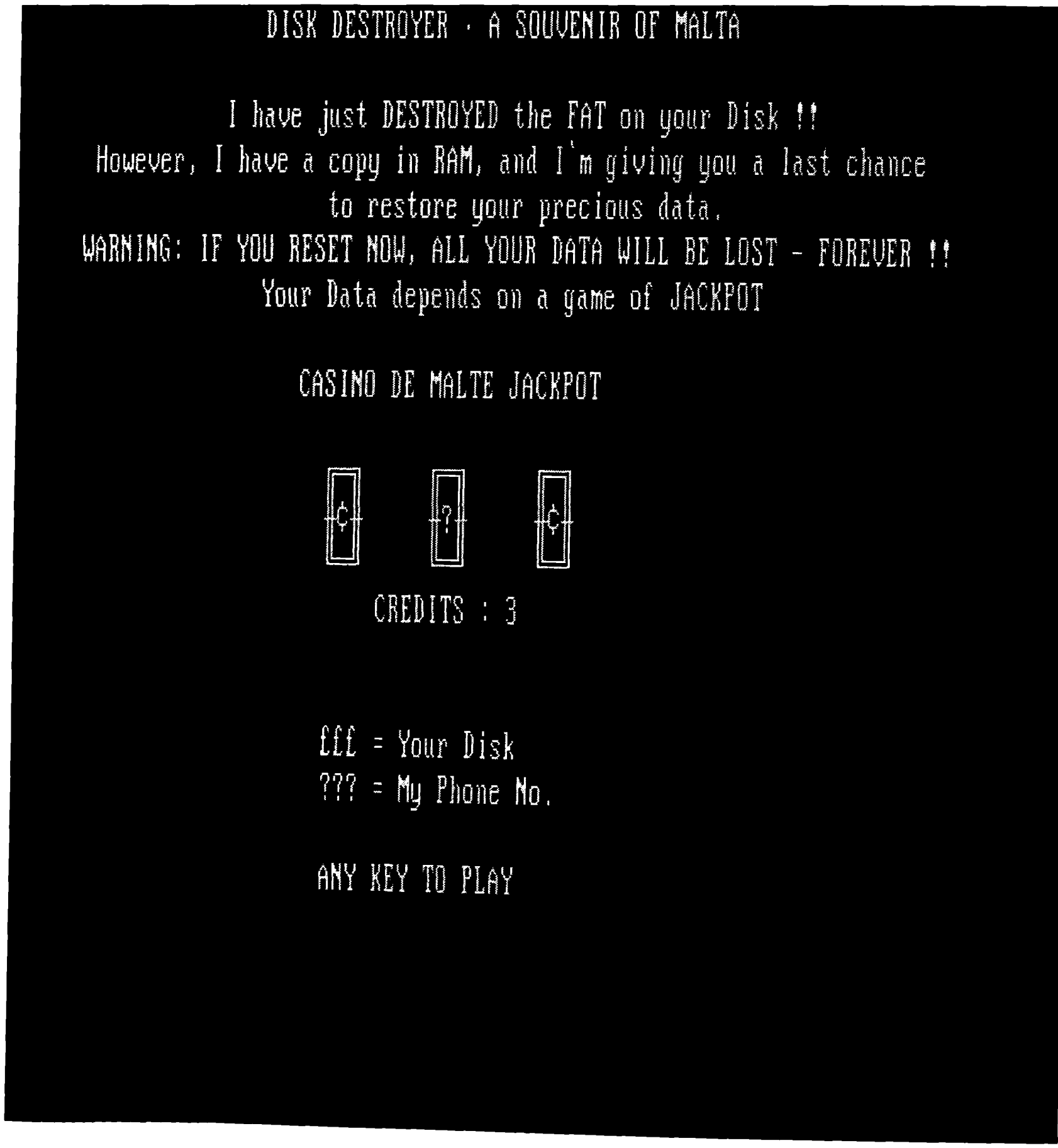
Ακολούθως απεικονίζονται ορισμένα παραδείγματα ιών που κυκλοφορούν στο Διαδίκτυο, τα οποία έχουν συλλεχθεί από τους παρακάτω δικτυακούς χώρους:

(Sophos Site)
http://www.sophos.com/pressoffice/imggallery/virusimg

(F-Secure Computer Virus Information Center).
http://www.f-secure.com/v-descs/

CASINO

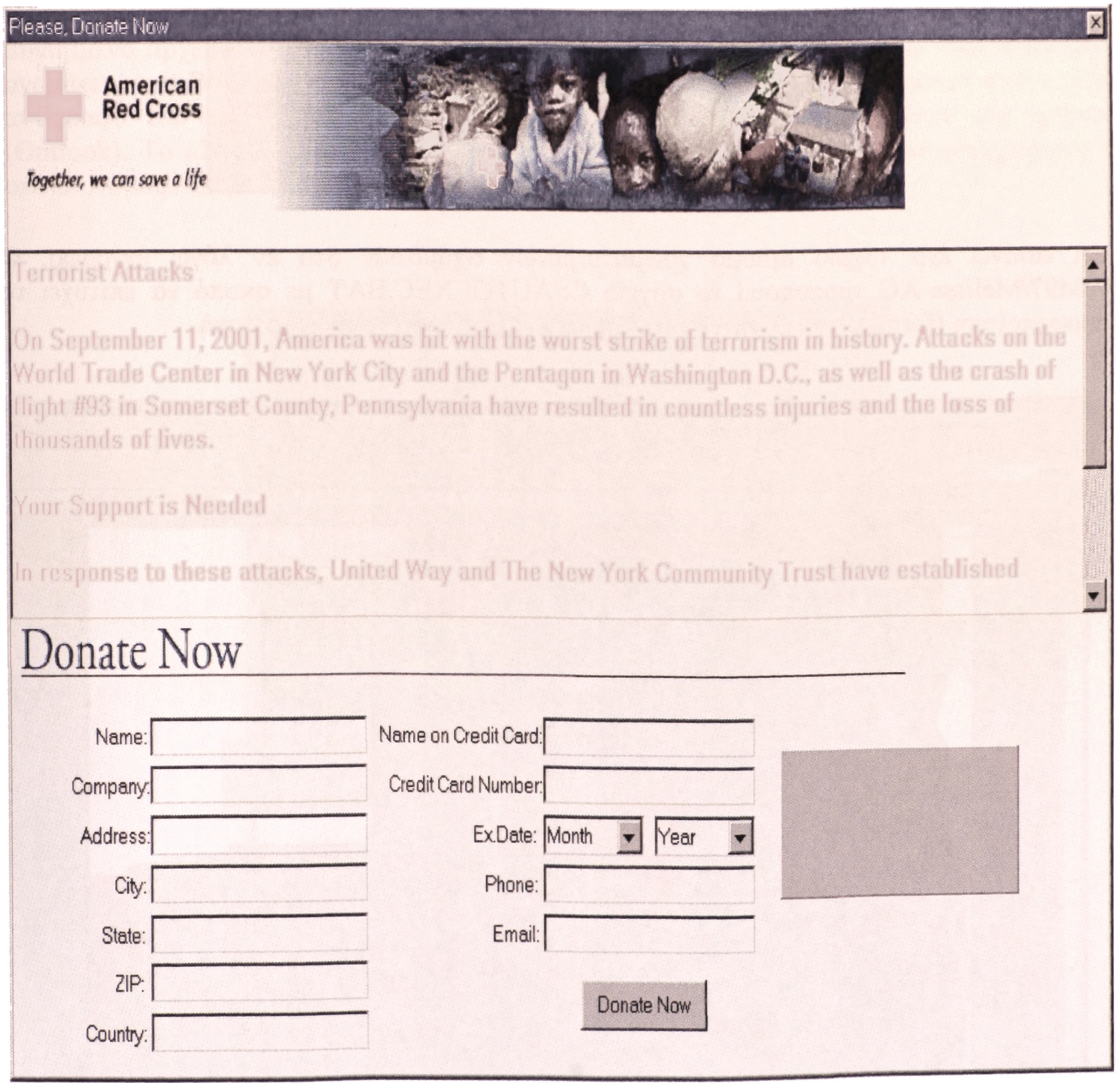
Ο **CASINO** είναι ένας πολύ σπάνιος ιός ο οποίος επιδεικνύει ένα μήνυμα που δείχνει ότι πρέπει να παίξετε ένα παιχνίδι Jackpot προκειμένου να σώσετε τα δεδομένα στον δίσκο σας.



Name: Casino
Type: Virus

TROJ/SEPTER

Ο **Troj/Septer** κλέβει πληροφορίες πιστωτικών καρτών προσποιούμενος ότι είναι μια online κυριότητα του Αμερικανικού Ερυθρού Σταυρού, παρουσιάζοντας μια επαγγελματική φόρμα η οποία θα πρέπει να συμπληρωθεί από τον χρήστη. Η φόρμα αυτή έχει πεδία για το όνομα του χρήστη, την εταιρεία, τη διεύθυνση, την πόλη, πολιτεία, το όνομα της πιστωτικής κάρτας, τον αριθμό της πιστωτικής κάρτας, την ημερομηνία λήξης, τον αριθμό τηλεφώνου και την ηλεκτρονική διεύθυνση.



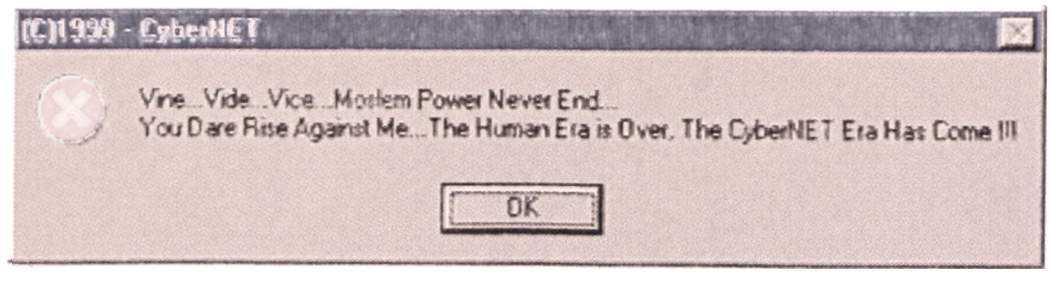
Name: Troj/Septer
Type: Trojan horse

WM97/Melissa-AG

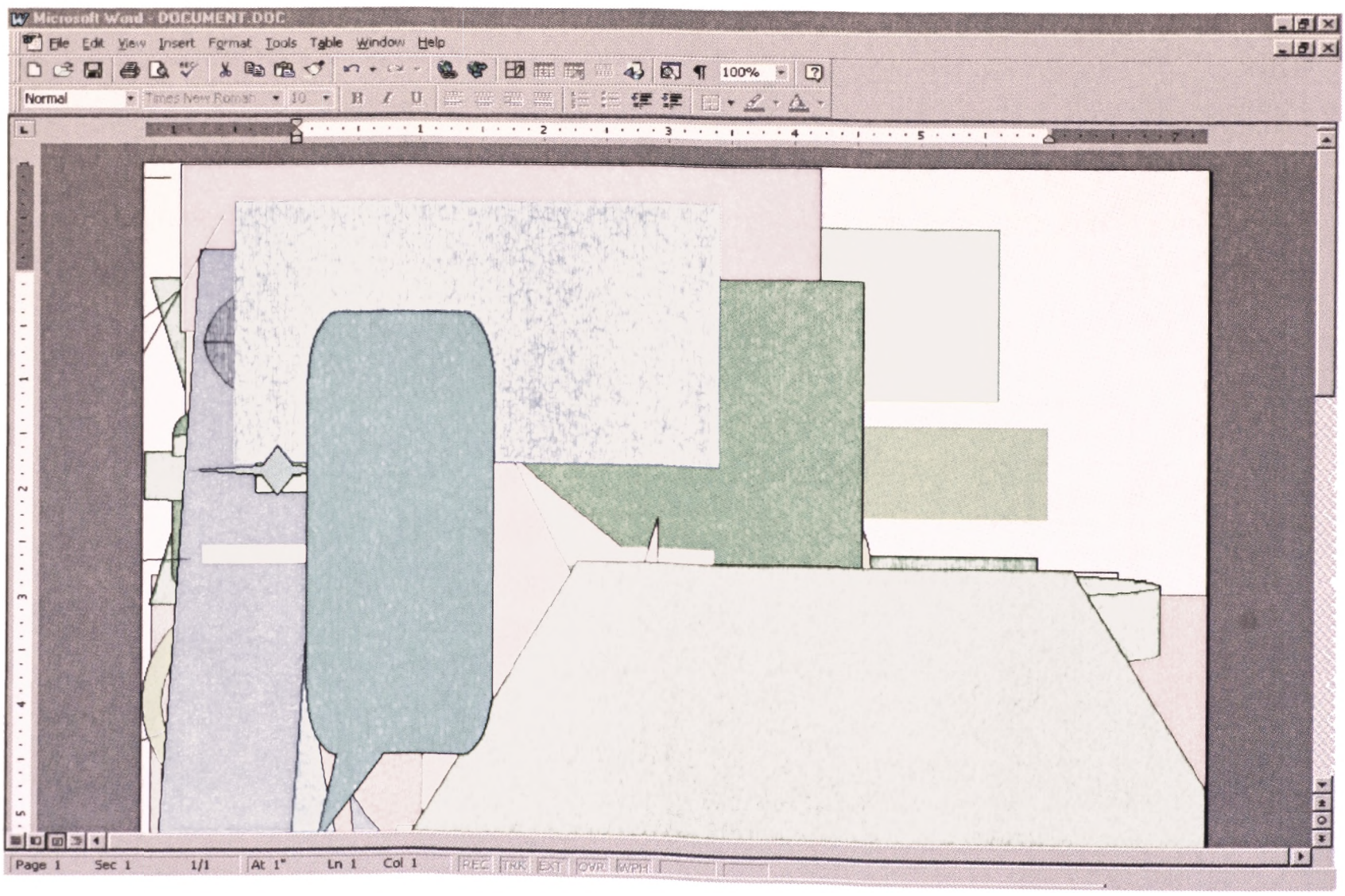
Ο **WM97/Melissa-AG** είναι μια μετάλλαξη του WM97/Melissa. Ο WM97/Melissa-AG στέλνει ένα αντίγραφο του μολυσμένου εγγράφου με μορφή συνημμένου στις 50 πρώτες καταχωρήσεις στο βιβλίο διευθύνσεων του χρήστη (Outlook). Το μήνυμα που στέλνει έχει τα ακόλουθα χαρακτηριστικά:

Subject message from <username>.
Message text: This document is very important and you've got to read this!!!

Ο ιός εμφανίζει ένα πλαίσιο κειμένου (όπως φαίνεται στο παρακάτω σχήμα)



και εισάγει ένα τυχαίο αριθμό χρωματισμένων σχημάτων στο εν λόγω έγγραφο. Ο WM97/Melissa-AG τροποποιεί το αρχείο C:/AUTOEXEC.BAT με σκοπό να επιτύχει τη μορφοποίηση (format) του C: drive όταν ξαναγίνει εκκίνηση του υπολογιστή.



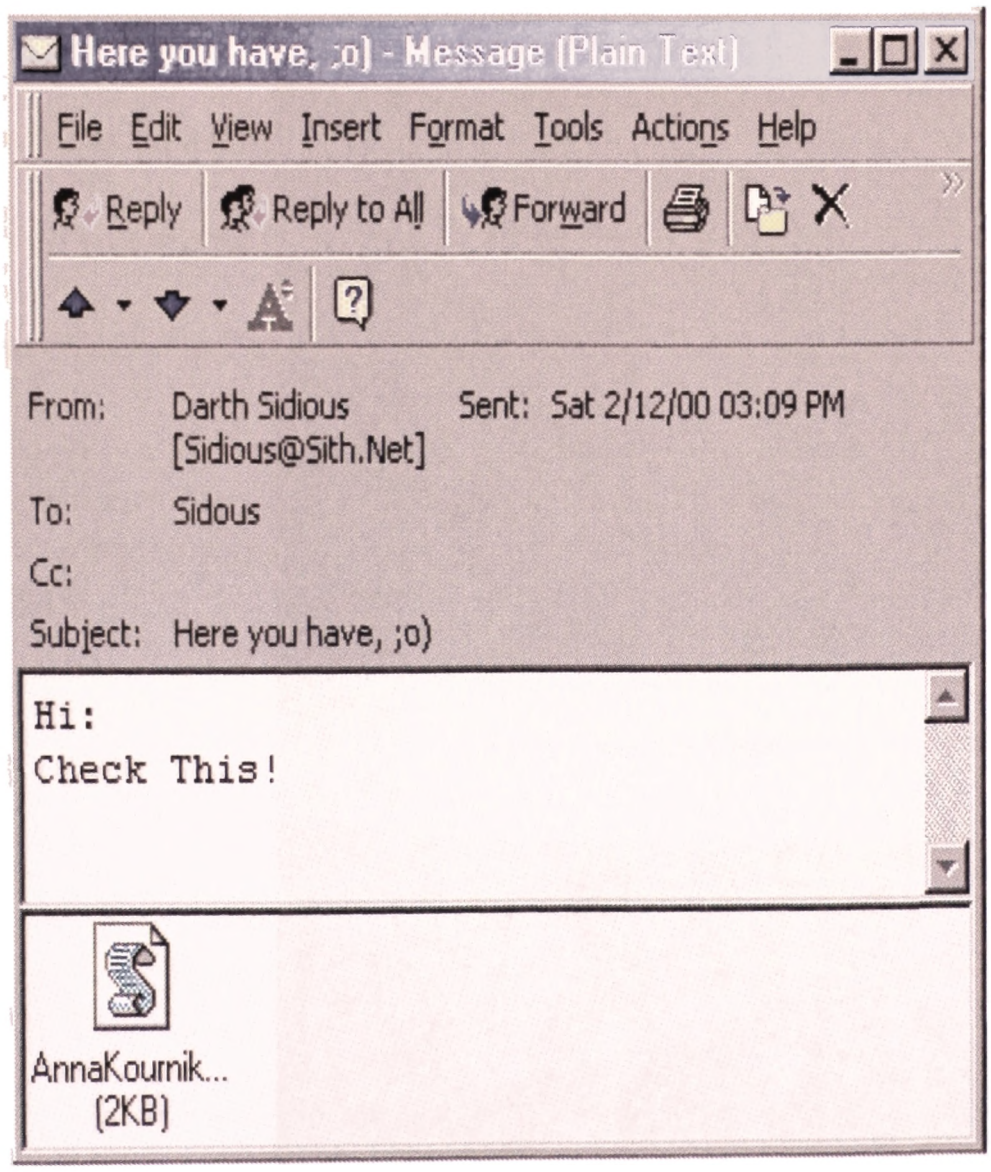
Name: WM97/Melissa-AG
Type: Worm

VBS/SST-A

Ο **VBS/SST-A** είναι ένα Visual Basic Script «Σκουλήκι» Ηλεκτρονικού Ταχυδρομείου. Το «Σκουλήκι» αφικνείται μέσω ενός ηλεκτρονικού μηνύματος (email) με τα ακόλουθα χαρακτηριστικά:

Subject line: here you have,;O)
Message text: hi: Check This!
File attachment: AnnaKournikova.jpg.vbs.

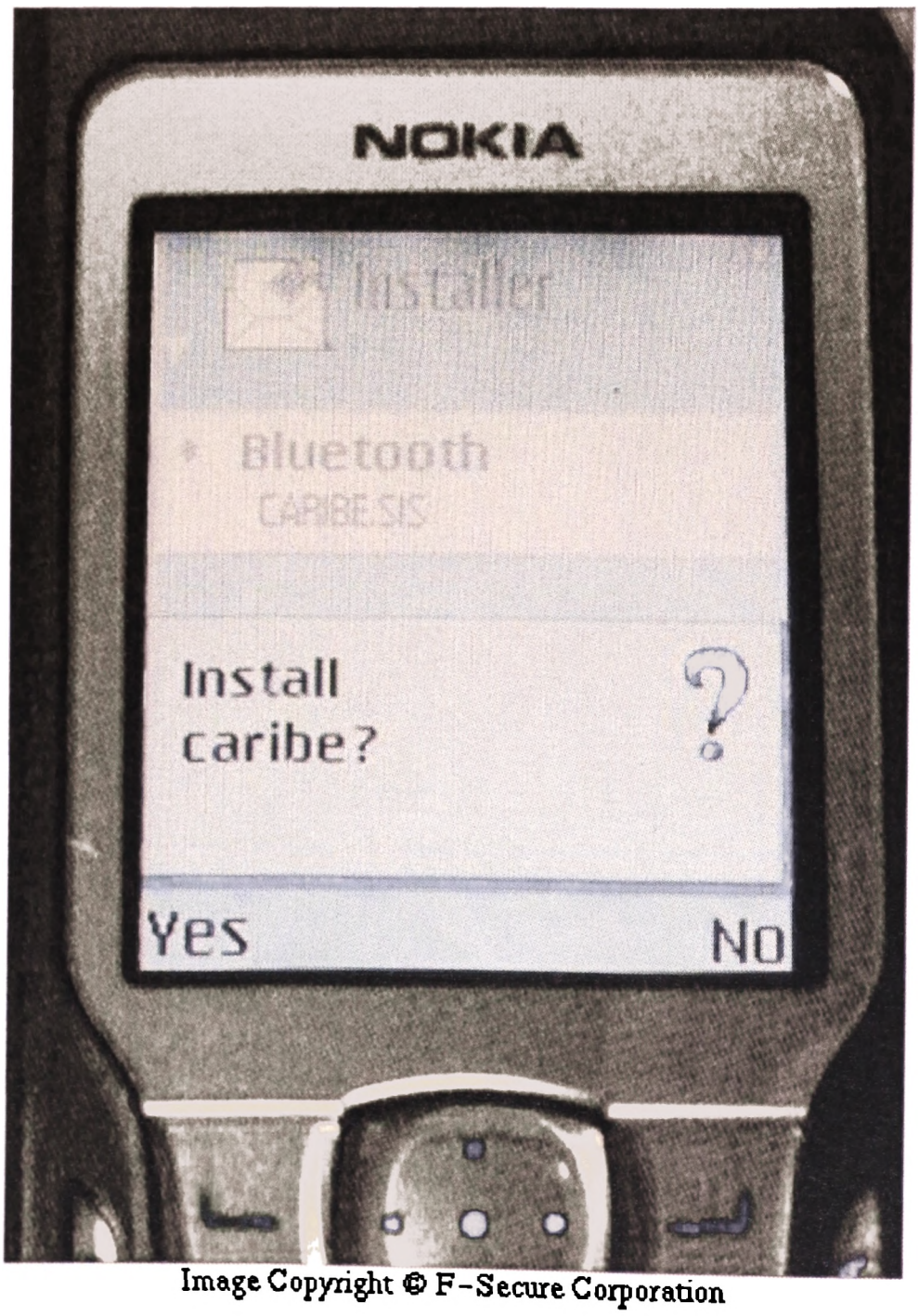
Το «Σκουλήκι» αυτό δελεάζει τους χρήστες να το ενεργοποιήσουν παριστάνοντας ότι είναι ένα γραφικό jpeg της Ρωσίδας τενίστριας Άννας Κουρνίκοβα. Την πρώτη φορά που το συνημμένο αρχείο θα εκτελεστεί, θα γράψει ένα αντίγραφο του εαυτού του στον κατάλογο ονομάτων των Windows του χρήστη. Το «Σκουλήκι» έπειτα θα προσπαθήσει να στείλει ένα αντίγραφο του εαυτού του σε κάθε καταχώρηση στο βιβλίο διευθύνσεων του χρήστη (Outlook). Το «Σκουλήκι» κάνει αλλαγές στο Registry, δημιουργώντας μια καταχώρηση η οποία ονομάζεται HKCU\software\OnTheFly.



Name: VBS/SST-A
Type: Worm

Mabir.A

Ο **Mabir.A** είναι ένα σκουλήκι το οποίο μολύνει κινητά τηλέφωνα και είναι ικανό να εξαπλωθεί μέσω Bluetooth και μέσω MMS. Όταν το σκουλήκι αυτό μολύνει ένα τηλέφωνο, ψάχνει για άλλα τηλέφωνα (μέσω της υπηρεσίας Bluetooth) και στέλνει μολυσμένα SIS αρχεία στα τηλέφωνα τα οποία βρίσκει. Ο Mabir.A αντιγράφεται μέσω της υπηρεσίας Bluetooth σε SIS αρχεία τα οποία πάντα ονομάζονται Carib.sis. Το αρχείο SIS περιέχει τα αρχεία caribe.app, caribe.rsc and flo.mdl τα οποία συνθέτουν τον Mabir.A. Το αρχείο SIS περιέχει ρυθμίσεις αυτόματης έναρξης (autostart) οι οποίες θα εκτελέσουν αυτόματα το αρχείο caribe.app, αφού πρώτα έχει εγκατασταθεί το αρχείο SIS. Με αυτόν τον τρόπο γίνεται η ενεργοποίηση του σκουληκιού. Όταν το σκουλήκι ενεργοποιηθεί, θα αρχίσει να ψάχνει για άλλες συσκευές που χρησιμοποιούν την υπηρεσία Bluetooth και θα αρχίσει να στέλνει τον εαυτό του στα πρώτα τηλέφωνα τα οποία βρίσκει. Εάν το στοχευόμενο τηλέφωνο βγει εκτός σειράς ή απορρίψει τη μεταφορά των αρχείων τότε το σκουλήκι θα προσπαθήσει πάλι να στείλει μηνύματα στο ίδιο τηλέφωνο.



Name: Mabir.A
Type: Worm

Ο Mabir.A επίσης αντιγράφεται μέσω MMS στέλνοντας MMS μηνύματα, τα οποία περιέχουν ένα μολυσμένο SIS αρχείο, σε άλλους χρήστες. Τα μηνύματα MMS περιέχουν το αρχείο Mabir SIS το οποίο ονομάζεται info.sis. Όταν στο μολυσμένο τηλέφωνο φτάσει ένα μήνυμα SMS ή MMS από κάποιον άλλο χρήστη, προκαλείται η ενεργοποίηση του Mabir, ο οποίος στέλνει τον εαυτό του σαν ένα MMS μήνυμα στον αριθμό από τον οποίο προήλθε το MMS ή το SMS. Με αυτό τον τρόπο ο Mabir προσπαθεί να εξαπατήσει τον δέκτη, προσποιούμενος ότι το MMS το οποίο στάλθηκε στον δέκτη αποτελεί απάντηση στο μήνυμα το οποίο νωρίτερα αυτός είχε στείλει στο μολυσμένο τηλέφωνο. Μόλις το αρχείο Mabir SIS (με όνομα αρχείου info.sis) εγκαθίσταται, το πρόγραμμα εγκατάστασης θα αντιγράψει τα εκτελέσιμα τμήματα του σκουληκιού στις ακόλουθες τοποθεσίες:

\system\apps\Caribe\Caribe.app

\system\apps\Caribe\Caribe.rsc

\system\apps\Caribe\flo.mdl

Όταν το αρχείο Mabir.exe εκτελείται, αντιγράφει τα ακόλουθα αρχεία:

\system\symbiansecuredata\caribesecuritymanager\Caribe.app

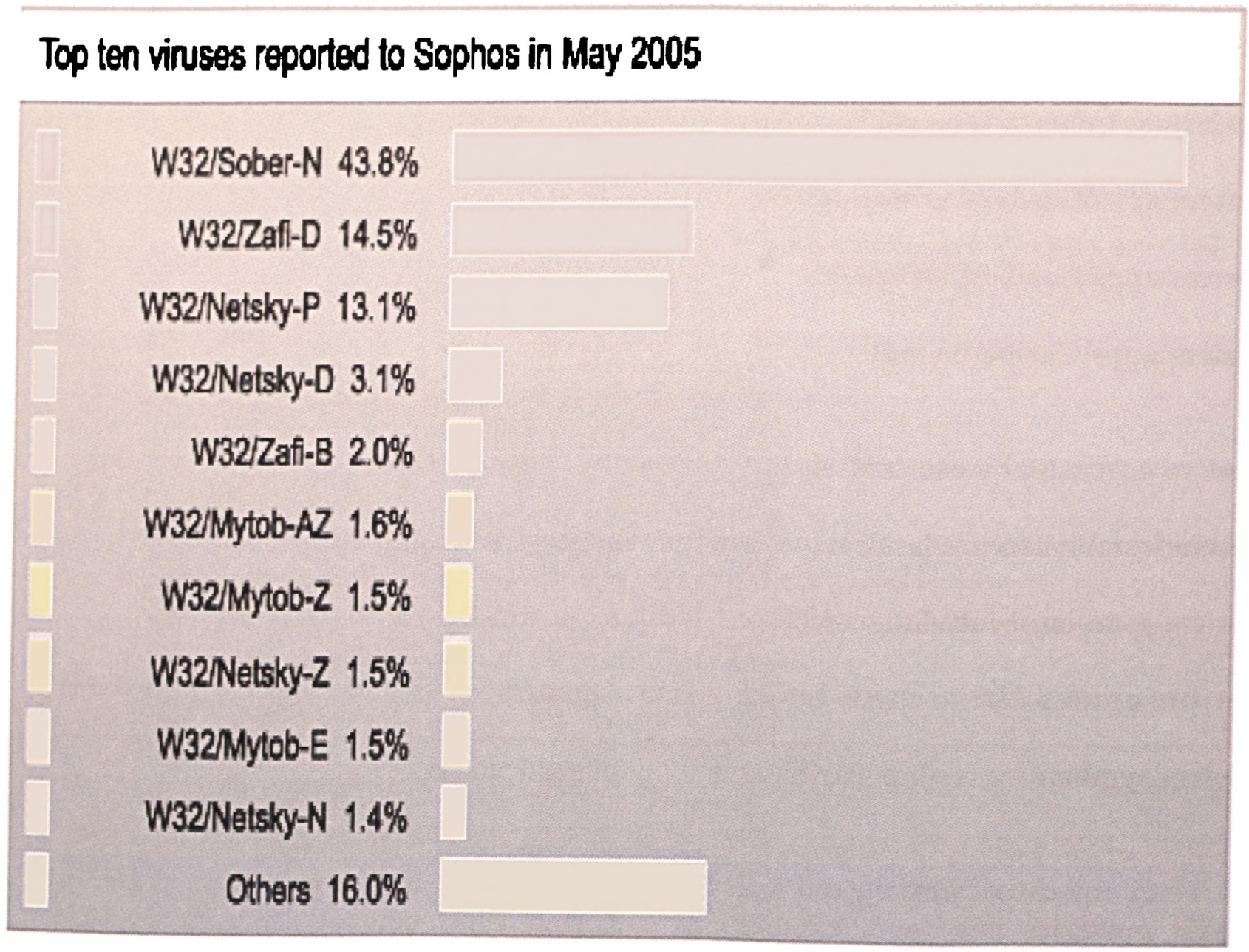
\system\symbiansecuredata\caribesecuritymanager\Caribe.rsc

Και ανακατασκευάζει το αρχείο SIS στην ακόλουθη τοποθεσία:

\system\symbiansecuredata\caribesecuritymanager\Info.sis

Μετά την ανακατασκευή του αρχείου SIS το σκουλήκι αρχίζει να ψάχνει για όλες τις ορατές συσκευές που χρησιμοποιούν την υπηρεσία Bluetooth και περιμένει την άφιξη μηνυμάτων SMS ή MMS.

Στο παρακάτω σχήμα απεικονίζονται οι δέκα κορυφαίοι ιοί οι οποίοι αναφέρθηκαν στον δικτυακό τόπο **SOPHOS** (**http://www.sophos.com**) τον Μάιο του 2005:



Source: Sophos Plc www.sophos.com

W32/Sober-N

Ο **W32/Sober-N** είναι ένας νέος ιός ο οποίος ανακαλύφθηκε στις 6 Απριλίου 2005 για τον οποίο έγιναν οι περισσότερες αναφορές (σύμφωνα με τον δικτυακό τόπο **SOPHOS**) τον Μάιο του 2005 (οι αναφορές σε ποσοστό φτάνουν το 43.8% των δέκα κορυφαίων ιών που αναφέρθηκαν). Ο W32/Sober-N είναι ένα σκουλήκι ηλεκτρονικού ταχυδρομείου το οποίο στέλνει τον εαυτό του, με μορφή συνημμένου αρχείου, σε διευθύνσεις τις οποίες υποκλέπτει από τον μολυσμένο υπολογιστή, περιέχοντας Αγγλικά ή Γερμανικά κείμενα. Το ηλεκτρονικό μήνυμα το οποίο στέλνει το σκουλήκι εξαρτάται από την διεύθυνση του παραλήπτη. Οι παραλήπτες των οποίων η ηλεκτρονική διεύθυνση είναι σε πεδία τύπου .de, .ch, .at, .li ή περιέχουν το αλφαριθμητικό "gmx." θα λάβουν ένα μήνυμα όπως φαίνεται παρακάτω:

Subject line:

Ihr Passwort
Mail-Fehler!
Ihre E-Mail wurdeverweigert
Ich bin's, was zum lachen :)
Glueckwunsch: Ihr WM Ticket
WM Ticket Verlosung
WM-Ticket-Auslosung
Ich habe Ihre E-Mail bekommen!

Message text:

Herzlichen Glueckwunsch,
Passwort und Benutzer-Informationen befindensich in der beigefuegten Anlage.
Diese E-Mail wurde automatisch erzeugt
Mehr Information finden Sie unter <URL>
Folgende Fehler sind aufgetreten:
Fehler konnte nicht Explicit ermittelt werden
End Transmission
Aus Datenschutzrechtlichen Gruenden, muss die vollstaendige E-Mail incl. Daten gezippt & angehaengt werden.
Wir bitten Sie, dieses zu beruecksichtigen.
Nun sieh dir das mal an!
--- FIFA-Pressekontakt:
beim Run auf die begehrten Tickets fnr die 64 Spiele der Weltmeisterschaft 2006 in Deutschland sind Sie dabei.
Weitere Details ihrer Daten entnehmen Sie bitte dem Anhang.
Mail-Scanner: Es wurde kein Virus festgestellt, AntiVirus: Kein Virus gefunden, AntiVirus-System: Kein Virus erkannt

Attached file:

Fifa_Info-Text.zip
OkTicket-info.zip
our_secret.zip

Τα συνημμένα ονόματα αρχείων ίσως να περιέχουν ένα προαιρετικό πρόθεμα τύπου "error-" ή μια επισυναπτόμενη κατάληξη τύπου "-Text" ακολουθούμενα με μια κατάληξη ZIP: Για παράδειγμα **our_secret-Text.zip.** Τα ηλεκτρονικά μηνύματα τα οποία στέλνει ο W32/Sober-N σε άλλες διευθύνσεις έχουν τα ακόλουθα χαρακτηριστικά:

Subject line:

Mailing error
Registration Confirmation
Your email was blocked
Your Password

Message text:

This is an automatically generated E-Mail Delivery Status Notification.
Mail-Header, Mail-Body and Error Description are attached
(See attached file: <zip file name>)

Account and Password Information are attached!
Visit: <URL>
*** AntiVirus: No Virus found
*** "<vendor name>" Anti-Virus
*** <vendor url>
(See attached file: <zip file name>)

Account and Password Information are attached!
Visit: <URL>
(See attached file: <zip file name>)

Account and Password Information are attached!
Visit: <URL>
*** Server-AntiVirus: No Virus (Clean)
*** "<vendor name>" Anti-Virus
*** <vendor url>
(See attached file: <zip file name>)

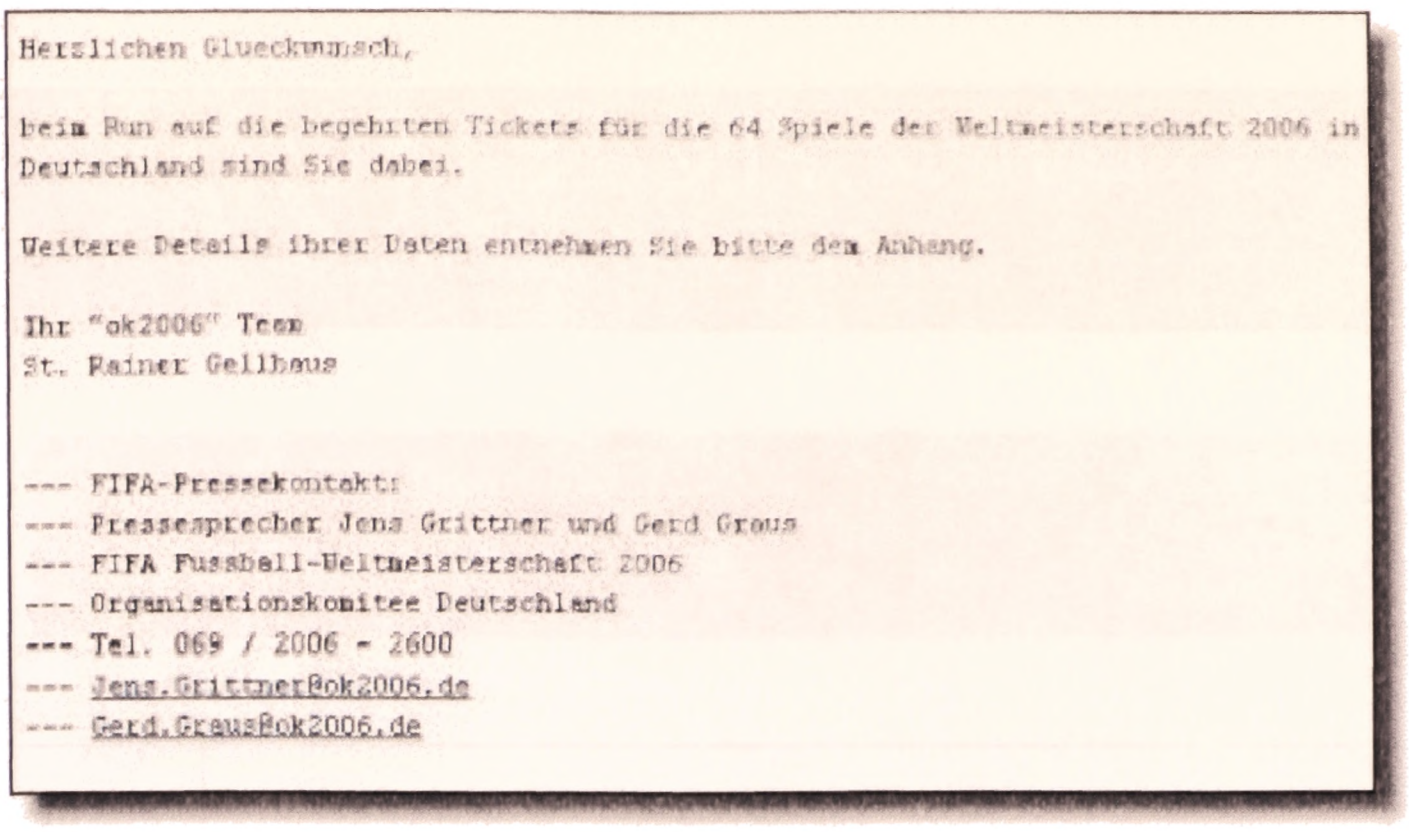
ok ok ok,,,,, here is it
*** AntiVirus: No Virus found
*** "<vendor name>" Anti-Virus
*** <vendor url>
(See attached file: <zip file name>)

Attached file:

mail_info.zip
account_info.zip
our_secret.zip

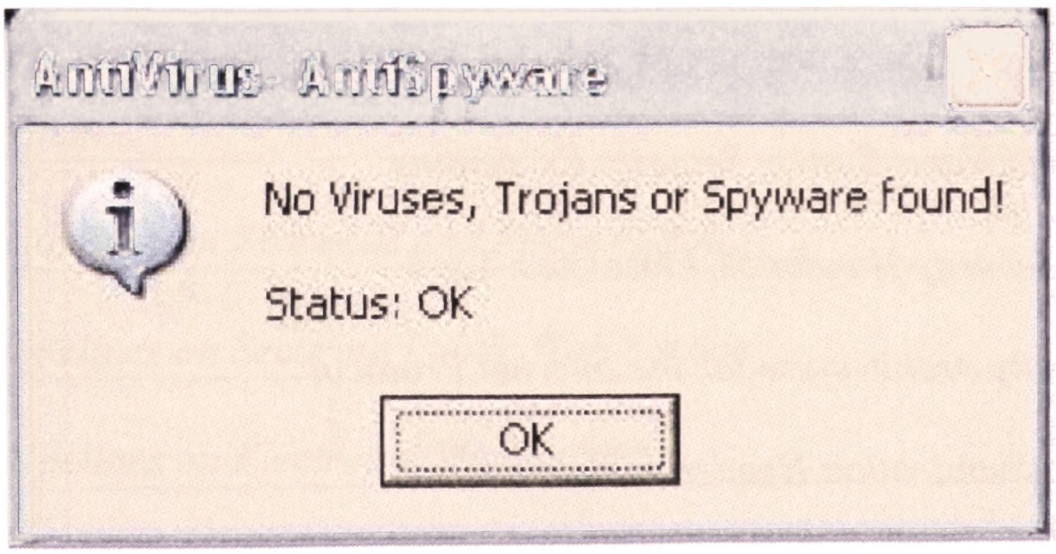
Τα συνημμένα ονόματα αρχείων ίσως να περιέχουν ένα προαιρετικό πρόθεμα τύπου "error-" ή μια επισυναπτόμενη κατάληξη τύπου "-Text" ακολουθούμενα με μια κατάληξη ZIP. Το αρχείο ZIP εμπεριέχει ένα εκτελέσιμο αρχείο το οποίο θα ονομάζεται **Winzipped-**

Text_Data.txt<spaces>.pif. Το παρακάτω σχήμα δείχνει ένα τυπικό μήνυμα το οποίο στέλνει το σκουλήκι W32/Sober-N.



```
Herzlichen Glueckwunsch,

beim Run auf die begehrten Tickets für die 64 Spiele der Weltmeisterschaft 2006 in
Deutschland sind Sie dabei.

Weitere Details ihrer Daten entnehmen Sie bitte dem Anhang.

Ihr "ok2006" Team
St. Rainer Gellhaus


--- FIFA-Pressekontakt:
--- Pressesprecher Jens Grittner und Gerd Graus
--- FIFA Fussball-Weltmeisterschaft 2006
--- Organisationskomitee Deutschland
--- Tel. 069 / 2006 - 2600
--- Jens.Grittner@ok2006.de
--- Gerd.Graus@ok2006.de
```

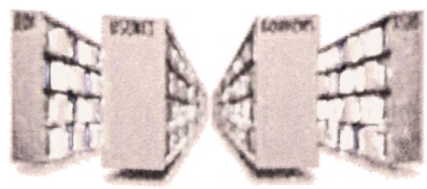
Ο W32/Sober-N προσπαθεί να εξουδετερώσει όλα τα προϊόντα προστασίας έναντι των ιών (Antivirus Products). Όταν το καταφέρει, το σκουλήκι αυτό ίσως να απεικονίσει ένα μήνυμα όπως φαίνεται στο παρακάτω σχήμα:



Name: W32/Sober-N
Type: Worm

ΠΑΡΑΡΤΗΜΑ Β

ΑΝΑΦΟΡΕΣ ΣΕ RFCs
(Request For Comment)



RFC NYMBER	TITLE	DATE
822	*Standard for the Format ARPA Internet Text Messages*	*August 1980*
1244	*Site Security Handbook*	*July 1991*
1636	*Security in the Internet Architecture*	*June 1994*
1825	*Security Architecture for the Internet Protocol*	*August 1995*
2065	*Domain Name System Security Extensions*	*January 1997*
2196	*Site Security Handbook,* Obsoletes: 1244	*September 1997*
2401	*Security Architecture for the Internet Protocol*	*November 1998*
2402	*IP Authentication Header*	*November 1998*
2406	*IP Encapsulating Security Payload*	*November 1998*
2408	*Internet Security Association and Key Management Protocol*	*November 1998*
2459	*Internet X.509 Public Key Infrastructure (Certificate and CRL Profile)*	*January 1999*

ΠΑΡΑΡΤΗΜΑ Γ

ΑΝΑΦΟΡΕΣ ΣΕ NIST SPECIAL PUBLICATIONS 800 SERIES

PUBLICATION NUMBER	TITLE	DATE
800-12	*An Introduction to Computer Security: The NIST Handbook*	
800-14	*General Accepted Principles and Practices for Securing Information Technology Systems*	*September 1996*
800-31	*Intrusion Detection Systems*	
800-34	*Contingency Planning Guide for Information Technology Systems*	*June 2002*
800-41	*Guidelines on Firewalls and Firewall Policy*	*January 2002*
800-44	*Guidelines on Securing Public Web Servers*	*September 2002*
800-45	*Guidelines on Electronic Mail Security*	*September 2002*
800-61	*Computer Security Incident Handling Guide*	*January 2004*
800-63 (Version 1.0.1)	*Electronic Authentication Guideline*	*September 2004*

ΠΑΡΑΡΤΗΜΑ Δ

ΒΙΒΛΙΟΓΡΑΦΙΑ

[Chap95] Brent D. Chapman & Elizabeth D. Zwicky, *Building Internet Firewalls,* First Edition, November 1995, O'Reilly Associates.

[Diff76] Diffie, W. and Hellman, M., *New Directions in Cryptography,* IEEE Transactions on Information Theory, November 1976.

[Kent98] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, November 1998.

[Shim02] Robert J. Shimonski, *Security +, Study Guide and DVD Training System,* copyright 2002 by Sungress Publishing, Inc.

[Stall99] William Stallings, *Cryptography and Network Security:* Principles and Practice, 2nd Edition. Upper Saddle River, NJ: Prentice Hall, 1999.

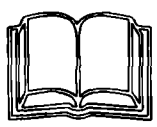
[Stall00] William Stallings, *Data and Computer Communications,* Sixth Edition, Published by Pearson Education, Inc, Publishing as Prentice Hall, 2000.

[Wood91] Charles Cresson Wood, *Corporate Security Policy,* October 1991.

[Zimm00] Philip R. Zimmermann, *the Official PGP Users Guide,* Edition Paperback, May 1995.

[Κομ02] Θεόδωρος Κομνηνός – Παύλος Σπυράκης, *Ασφάλεια Δικτύων Υπολογιστικών Συστημάτων: Αναχαιτίστε τους εισβολείς,* Σειρά: Τεχνολογία Πληροφορικής & Επικοινωνιών, Εκδόσεις «ΕΛΛΗΝΙΚΑ ΓΡΑΜΜΑΤΑ», 2002.

[Πομ03] Πομπόρτσης Αντρέας - Παπαδημητρίου Γεώργιος, *Ασφάλεια Δικτύων Υπολογιστών,* Εκδόσεις Τζιολα, 2003.



ΕΛΛΗΝΙΚΟ ΕΥΡΕΤΗΡΙΟ

A

B

Γ

Δ

Ε

Ζ

Η

Θ

Ι

Κ

Λ

Μ

Ν

Ξ

Ο

Π

Ρ

Σ

Τ

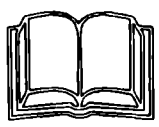
Υ

Φ

Χ

Ψ

Ω



ΑΓΓΛΙΚΟ ΕΥΡΕΤΗΡΙΟ

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z